UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

(Versão Pública)

REVISÃO DA ORGANIZAÇÃO DA INFRAESTRUTURA DE REDE DE CIÊNCIAS

Mestrado em Segurança Informática

João Filipe Santos Matias

Dissertação orientada por:
Prof. Doutor Hugo Alexandre Tavares Miranda
Pedro Miguel Raminhos Ribeiro Botas

2016

Agradecimentos

Quero agradecer aos meus orientadores, Professor Doutor Hugo Miranda e Pedro Botas pela disponibilidade e por todos os ensinamentos transmitidos.

Gostaria de deixar o meu especial agradecimento à minha família e amigos, pelo apoio e incentivo que me deram ao longo dos últimos meses e por estarem sempre presentes.

Quero ainda agradecer ao António Broega e Susana Pereira, que estiveram sempre disponíveis para ajudar.

Aos meus pais

Resumo

Um bom parque informático com uma rede eficiente e segura associada garante, aos utilizadores, a salvaguarda da sua informação e a facilidade de acesso aos serviços. Estes serviços são coordenados pelos administradores de rede e sistemas, onde o conhecimento de todos os recursos que gerem contribui para a resolução rápida e eficaz dos problemas que inevitavelmente vão surgindo.

Este trabalho contribui para aprofundar o conhecimento da rede da Faculdade de Ciências da Universidade de Lisboa, tentando não só, documentar a rede de forma a saber localizar todos os recursos de modo adequado e atempado, mas também encontrar eventuais problemas de configuração existentes. Isto irá permitir otimizar a rede da instituição de modo a melhorar a experiência de utilização para o cliente final, que no caso de Ciências, são principalmente os alunos, docentes, investigadores e funcionários.

Deste trabalho irão também surgir um conjunto de documentos dirigidos não só aos utilizadores da rede disponibilizada, mas também aos utilizadores de Ciências no geral.

Palavras-chave: Ciências, rede, administração

Abstract

A good IT facility based on an efficient and secure network ensures to the users the safety of their information, and also that the services made available by the institution are easy to access, which are coordinated by system and network administrators. This contributes for a better knowledge of the resources that this administrators manage and if some issue occurs, allows to quickly and effective fix it without the final user realize that the system has some kind of problem.

The goal of this work is to review the network infrastructure of Faculty of Sciences of the University of Lisboa, documenting this network so that administrators can have the knowledge of every resource managed by them and also detect possible anomalies. This will allow the improvement of the network, meaning that users, mainly students, teachers, investigators and employees, can make a better use of the systems.

From this work will also emerge a set of documents, addressed not only to the network users but also to the users of this institution in general.

Keywords: Administrator, Network, Ciências

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Motivação

A motivação original para este trabalho tem como base a necessidade de atualizar a documentação da rede de dados de Ciências, assim como fazer um levantamento da sua situação e a procura de soluções para algumas limitações observadas e bem conhecidas que restringem a qualidade dos serviços fornecidos aos utilizadores.

1.2 Objectivos

O objetivo deste relatório é melhorar a documentação, aumentar a eficiência e eficácia da gestão da infraestrutura da instituição, e ainda a resiliência e segurança dos dados dos utilizadores e serviços. Existe também a necessidade de expor falhas e configurações incorretas que de alguma forma afetem o desempenho, funcionalidade e segurança dos serviços.

Por fim, é ainda importante realçar a importância da criação de métodos que facilitem a identificação de problemas na rede e a prospeção de informação.

1.3 Contribuições

Através da elaboração de documentação que contribua para a melhoria dos processos de gestão das várias atividades de Ciências, foi possível aprofundar o conhecimento acerca da infraestrutura tecnológica de Ciências. Permitiu ainda a identificação e correção de problemas existentes que não eram conhecidos, tais como vulnerabilidades do tipo XSS e CSRF.

Adicionalmente, foram redigidos um conjunto de documentos que não existiam anteriormente com o objetivo principal de sensibilizar utilizadores em matéria de segurança informática e para os preparar para possíveis situações de emergência. Os

documentos redigidos foram Políticas de Segurança de Informação, Procedimentos de Segurança e Plano de Contingência.

1.4 Estrutura do documento

Este documento está organizado da seguinte forma:

Capítulo 2 – Enquadramento. É apresentada uma breve descrição da instituição.

Capítulo 3 – Arquitetura da rede de Ciências, onde é descrita a rede da instituição, problemas encontrados e respetivas soluções, assim como sugestões de melhorias.

Capítulo 4 – Administração de sistemas de Ciências, onde são identificadas vulnerabilidades na rede e sugeridas algumas correções. São ainda apresentadas as ferramentas de monitorização e alarmística existentes, assim como descritas as alterações às configurações SSL para websites e correio eletrónico.

Capítulo 5 – Regulamentação e formalização de procedimentos. São apresentados regulamentos que os utilizadores de Ciências têm que ter acesso e principalmente compreender, para que fiquem sensibilizados em matérias de segurança e proteção de informação, para uma consequente proteção da imagem da instituição.

Capítulo 2

Enquadramento

A Faculdade de Ciências da Universidade de Lisboa é uma instituição de ensino universitário público, criada a 19 de Abril de 1911. No centro da sua atividade estão o ensino e investigação científica. A organização é responsável por assegurar as melhores condições possíveis para o desenvolvimento de competências, tais como a disponibilização de espaços e equipamentos que satisfaçam as necessidades não só dos alunos e investigadores, como também de todas as entidades que possam interagir com a instituição. O campus desta instituição está dividido por 11 edifícios que albergam os diferentes departamentos e unidades de serviço de Ciências, cada um com necessidades específicas. No ano letivo de 2014/2015 a instituição prestou serviços a cerca de 5000 alunos, 400 docentes, 50 investigadores e 160 funcionários.

Ao nível dos sistemas de informação, Ciências fornece um conjunto variado de serviços, alguns dos quais requerem uma alta taxa de disponibilidade - como por exemplo a difusão de eventos na Internet (Streaming) -, razão pela qual são necessárias não só, precauções para garantir tal propriedade, mas também uma gestão cuidada do parque informático e um conjunto de equipamentos adequados ao bom funcionamento desta rede. A Direção de Serviços Informáticos (DSI) é a unidade de serviço responsável pela administração do parque informático de Ciências, que inclui cerca de 2000 máquinas ligadas à rede com fios, assim como pela gestão da rede sem fios à qual se ligam cerca de 1500 dispositivos diariamente. É ainda responsável pelo suporte a todos os seus utilizadores, o que inclui a resolução de problemas relacionados com contas e configuração de equipamentos a pedido de docentes, investigadores e alunos.

Este documento apresenta o trabalho desenvolvido no levantamento detalhado do atual estado da rede de Ciências. Adicionalmente, propõe e discute as mudanças desejáveis ao nível da organização da arquitetura de rede, e sobretudo os objetivos desta

mudança nomeadamente a melhoria da qualidade de serviço e a redução do esforço de administração.

Capítulo 3

Arquitetura da Rede de Ciências

3.1 Núcleo da Rede

A ligação entre Ciências e a Internet é assegurada pela Divisão de Serviços Informáticos da ULisboa. Do conjunto de seis pares de fibra ótica que materializam esta ligação, dois pares de fibra ótica (um de redundância) são utilizados para o tráfego de dados dos serviços de Ciências, um outro par é utilizado para serviços fornecidos no campus de Ciências, nomeadamente a rede sem fios. Os restantes pares de fibra estendem a rede de Ciências ao centro de dados da reitoria onde está alojada a réplica de armazenamento primário de Ciências, sendo que dois estão ligados em Fiber Channel (um de redundância) e o último assegura o serviço NAS.

Ciências utiliza os serviços da SIBS para permitir transações monetárias (por exemplo, para pagamento de propinas), pelo que é requisito desta empresa que a instituição tenha uma ligação de rede a uma operadora nacional, neste caso a NOS.

A separação entre a rede de Ciências e a ULisboa é feita através de uma Firewall Juniper (Série SRX3600), capaz de suportar cerca de 175000 novas ligações por segundo (sem perder nenhum pacote) e permite um máximo de 40000 políticas de segurança ativas e que funciona também como gateway. Esta solução é um conjunto ativo/passivo de firewall tolerante a falhas, constituído por dois chassis, um em modo ativo e outro em modo passivo. O nó ativo é responsável por processar todo o tráfego proveniente da ULisboa para Ciências (e vice-versa), enquanto o nó passivo apenas monitoriza o estado do nó ativo, para que no caso do nó ativo ficar offline, o possa substituir. Neste relatório esta solução vai ser referida apenas como Firewall. É importante mencionar que a sua configuração é feita ao longo de 27000 linhas, onde existem alguns problemas, visto que existem políticas mal definidas e contraditórias, como por exemplo políticas nomeadas *default_DENY_APAGAR* que têm como ação

permitir tráfego. Existem ainda objetos nesta configuração que concretizam a mesma regra, como é o caso dos objetos *Old_Inside_Hosts_C5_1* e *Old_Net_10.101.25.0/24*, dentro da zona da Firewall *Old_Inside_Hosts*, e que ambos representam a mesma rede, 10.101.25.0/24. Existem ainda 15 políticas de IDP existentes nesta Firewall, sendo que apenas uma está ativa.

Foram criadas 156 interfaces VLAN nesta Firewall com diversas finalidades e associadas a redes descritas detalhadamente mais à frente. A Firewall define ainda 34 zonas que agregam várias redes com políticas de segurança semelhantes.

Desta firewall sai um trunk[1] com todo o tráfego filtrado para um par de comutadores de rede (do inglês "switch") Cisco Nexus (Série 5596UP)[2] em barramento, responsáveis por distribuir todo o tráfego pelas 96 portas existente. As tramas (do inglês "frame") provenientes deste comutador são identificadas através da norma 802.1Q que adiciona 4bytes ao cabeçalho da trama original, para identificar a VLAN a que se destina a trama. O protocolo 802.1Q permite um máximo de 4094 VLANs, o que no caso de Ciências é suficiente. A utilização deste método permite assim a distribuição de tráfego por máquinas pertencentes a diferentes VLANs por todo o campus da faculdade utilizando um único meio físico. A rede utiliza o protocolo PVST+ que destina regras de encaminhamento de nível 2 (ligação de dados) independentes por VLAN, utilizando para tal uma instância de Spanning Tree por VLAN. Os protocolos de Spanning Tree são fundamentais em cenários onde existe redundância nas ligações entre comutadores por evitarem a ocorrência de ciclos dentro da rede sem prejudicar a tolerância a faltas oferecida pela redundância.

[1] Notação Cisco referente a links que transportam tráfego de várias VLANs sobre um único link e que permitem distribuir uma VLAN pela rede, isto é, distribuí-la por vários comutadores de rede.

[2] O Nexus 5596UP é um comutador de rede composto por duas racks capaz de encaminhar 1428 mpps (Camada 2 OSI) e 240 mpps (Camada 3 OSI). Este comutador tem 48 portas.

3.2 Camada Ligação de Dados

A análise realizada, que incluiu o levantamento dos equipamentos existentes, identificou 112 comutadores de rede administrados pela DSI e geograficamente distribuídos pelo campus de Ciências a que correspondem aproximadamente 4000 portas de comutador para atribuição. De referir que este valor não corresponde ao total de comutadores existentes, pois alguns departamentos possuem equipamentos próprios, sendo responsáveis pela sua administração. Estes equipamentos não são tidos em conta na análise apresentada neste documento.

Na Figura 1 é apresentada a distribuição de comutadores pelos diferentes edifícios da instituição.

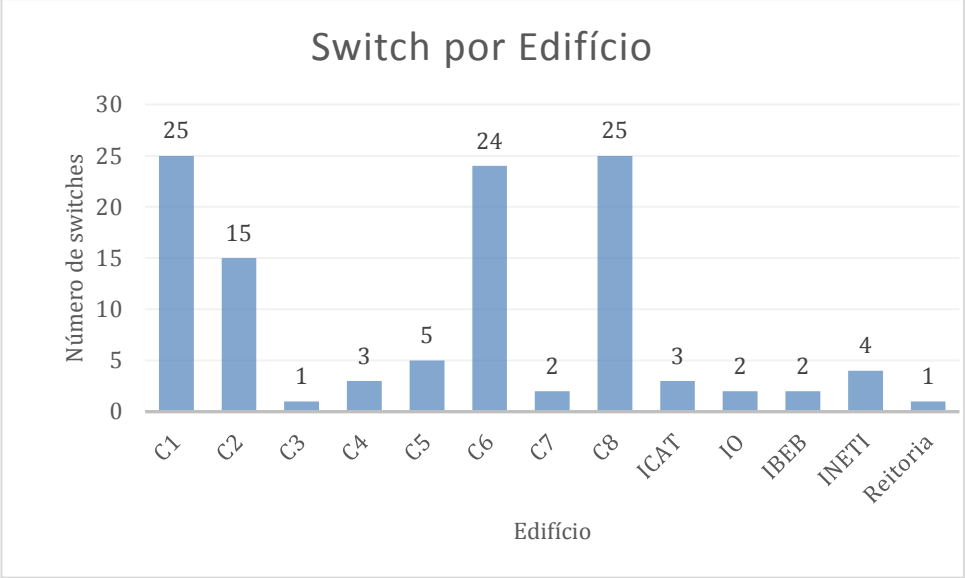


Figura 1: Distribuição de equipamentos de Nível 2 (Comutadores) pela Faculdade

Da Figura anterior, destaca-se o C1 com maior número de comutadores, facilmente justificado pelo alojamento do datacenter e por ser onde existem mais laboratórios e salas com computadores para utilização dos alunos. Seguem-se os edifícios C6 e C8, com número elevado de comutadores quando comparado com outros edifícios, devido às grandes dimensões, por serem os que alojam o maior número de docentes e investigadores.

A Figura 1 evidencia a distribuição dos números de comutadores por modelo. Todos os equipamentos existentes são Cisco. Esta homogeneidade é uma opção da DSI que tem como objetivo simplificar as tarefas de administração e a interoperabilidade dos equipamentos.

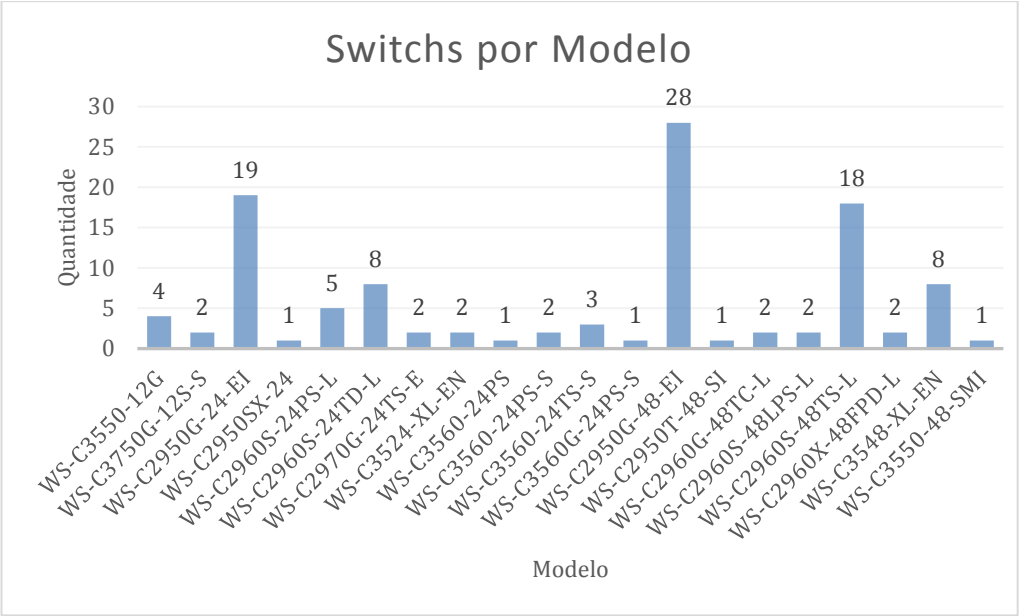


Figura 2: Distribuição de equipamentos por modelo (Cisco)

Como foi possível perceber desde o início deste estudo, um dos principais pontos fracos da infraestrutura tecnológica de Ciências são os comutadores de rede, equipamentos demasiado antigos e que não são capazes de satisfazer os atuais requisitos da instituição.

Cruzando a informação da Tabela 1 com a Figura 2 é possível perceber que a maioria dos comutadores de rede suporta um máximo de 64 instâncias STP, o que é bastante inferior ao número de VLANs existentes, pelo que o comutador tem de fazer a gestão das VLANs ativas e proceder à desativação do protocolo STP para algumas VLANs. Esta é a raiz do problema dos comutadores esgotarem a memória que possuem.

Modelo do Comutador (Cisco)	Nº Máximo Instâncias STP	Nº Máximo VLANS
2950 EI / 2960 EI	64	250
3550 / 3560 / 3750	128	1005

Tabela 1 : Instâncias STP e VLANs por Modelo de Comutador Cisco

Note-se que este é essencialmente um problema de caráter financeiro, pois a solução ideal passaria por adquirir comutadores mais recentes comparando com os atuais, capazes de suportar as atuais necessidades da instituição.

Visto que tal não é possível, resta fazer a melhor gestão possível dos equipamentos disponíveis, fazendo uma monitorização adequada para detetar eventuais problemas que possam surgir, e ajustando a configuração de cada comutador sempre que possível de

forma a maximizar a sua eficácia. Devem ser adquiridos novos equipamentos gradualmente para substituir os mais antigos, para que a questão dos comutadores sem memória seja mitigada.

Da análise dos nomes de todos os comutadores de Ciências é possível perceber que duas notações predominam, {EDIFICIO}_B{Nº BASTIDOR|LETRA BASTIDOR}_#{Nº SWITCH} para 85 dos 112 comutadores existentes e DATACENTER_B{Nº FILA}.{Nº BASTIDOR}_#{Nº SWITCH} para 13 comutadores. Na primeira notação, aos bastidores dos edifícios C2 e C8 não foram atribuídos números, mas sim letras devido à organização ser feita por zonas que derivam da construção dos edifícios e que justifica os nomes serem diferentes. Na segunda notação, estão incluídos grande parte dos comutadores alojados no datacenter da instituição. Os restantes comutadores da instituição não seguem nenhuma desta notação.

Posto isto, foi apresentada uma proposta para uniformizar o nome de todos os comutadores da instituição, sendo que notação usada para o datacenter foi mantida. A notação proposta, {EDIFICIO}_B{Nº PISO}.{Nº BASTIDOR}_#{Nº SWITCH}, veio substituir a anteriormente apresentada, facilitando a localização de cada comutador e veio também abranger todos os restantes que não seguem qualquer norma. De referir que existiam alguns comutadores de rede no datacenter que não seguiam nenhuma norma, pelo que foram incluídos na notação do datacenter. Note-se que esta solução não é de execução trivial, pois não se trata de "apenas" mudar o nome dos comutadores, mas sim, alterar os mapas de rede, as configurações de clientes SSH usados para aceder remotamente aos dispositivos e ainda, alterar a base de dados de administração de tomadas. As tomadas dos edifícios têm nomes atribuídos consoante as zonas a que pertencem pelo que todas as tomadas de rede, por exemplo do C2 e C8, teriam que ser renomeadas, assim como todas as descrições das portas dos comutadores destes edifícios. Note-se ainda que esta solução não representa uma melhoria ao nível do desempenho da rede de Ciências, mas sim ao nível da documentação e do fácil acesso à informação.

O Mapa de Rede de Nível 2, onde são evidenciadas as interligações básicas de todos os comutadores administrados pela DSI é apresentado no Anexo A

Semelhante a este problema temos os identificadores das VLANs, que aparentemente não têm nenhuma norma para identificação, à exceção de algumas redes da gama 10.101, em que o identificador da VLAN corresponde ao terceiro conjunto de bits do IP da rede associada a essa VLAN. Este é um problema que tem impacto no

acesso intuitivo à informação, neste caso aos recursos, e a sua resolução através de uma convenção bem definida é apenas uma questão de organização.

3.3 Camada Rede

Ciências foi a primeira faculdade da ex Universidade de Lisboa a ter ligação à Internet, sendo que lhe foi atribuída a gama de endereços 194.117.0.0-194.117.49.255. Os endereços entre 194.117.24.0 e 194.117.39.255 foram mais tarde cedidos ao INESC, que ainda é responsável por essas gamas de IPs. É importante perceber que nessa época, a instituição possuía poucas máquinas e todas tinham IP público, pelo que mais tarde, e com o aumento da rede, foi necessário criar uma rede privada.

A equipa que planeou tal alteração, não a limitou apenas à faculdade de Ciências, mas sim a toda a Universidade de Lisboa (antes da fusão com a UTL), pelo que era necessária uma gama de endereços capaz de hospedar todas as máquinas. Das três gamas de redes privadas existentes, a rede *10.* é a que permite mais endereços (rede classe A com 8 bits de máscara) logo, era a única escolha possível. A equipa responsável por esta implementação definiu ainda que as gamas de endereços a atribuir seriam a *10.100.* para a ex-ULisboa (Reitoria), a *10.101* para Ciências, a *10.102* para a Faculdade de Psicologia e Ciências da Educação, e assim sucessivamente. Ciências ficou assim, com a rede 10.101.0.0/16 para uso interno que ainda hoje é usada.

Existia agora a necessidade de traduzir os endereços internos para externo, de forma a terem acesso à rede pública, pelo que foi implementado o NAT, responsável por fazer tal tradução, e que basicamente mantém uma tabela de correspondências entre endereços privados e públicos (1 para 1). De forma a fazer uso de menos endereços públicos, pois atualmente existem poucos disponíveis, foi implementado o PAT, uma extensão do NAT, que permite mapear vários endereços privados num único endereço público, através da manipulação de portos.

Aliado a isto, Ciências ficou ainda, através de um acordo com a ULisboa, com a rede *10.121.0.0/16*, que atualmente está em uso no Datacenter de Ciências e que permite fazer uma separação entre estas máquinas e máquinas terminais, isto é, máquinas de utilizadores. Tal separação é percetível mais abaixo.

Assim, Ciências utiliza encaminhamento baseado em tabelas estáticas, numa topologia em estrela centralizada na Firewall, pelo que não é utilizado qualquer equipamento para encaminhamento ao nível de rede.

Esta secção descreve todas as redes existentes em Ciências.

Redes dos Docentes

Neste grupo incluem-se todas as redes dedicadas aos docentes, onde estão ligadas as máquinas dos gabinetes.

- 10.101.60.0/24, 10.101.69.0/24, 10.101.73.0/24, 10.101.76.0/24, 10.101.80.0/24, 10.101.88.0/24, 10.101.93.0/24, 10.101.96.0/24, 10.101.97.0/24, 10.101.49.0/24, 10.101.64.0/24 e 10.101.65.0/24.

Correspondem, respetivamente, ao Departamento de Engenharia Geográfica, Geofísica e Energia, Departamento de Biologia Animal, ao Departamento de Estatística e Investigação Operacional, ao Departamento de Educação, ao Departamento de Geologia, ao Departamento de Matemática, ao Departamento de Química e Bioquímica, ao Departamento de Física (duas gamas de endereços) e ao Departamento de Informática e Departamento de Biologia Vegetal (duas gamas de endereços).

Redes dos Investigadores

Aqui estão agrupadas as redes usadas pelos investigadores. Este grupo de utilizadores não é incluído nas redes dos docentes, ou mesmo dos alunos devido às diferentes necessidades deste grupo e diferentes tipos de permissões.

- 10.101.126.0/24, 10.101.130.0/24, 10.101.134.0/24, 10.101.137.0/24, 10.101.146.0/24, 10.101.154.0/24, 10.101.158.0/24 e 10.101.162.0/24

Redes das máquinas das salas disponibilizadas aos investigadores do Departamento de Engenharia Geográfica, Geofísica e Energia, do Departamento de Biologia Vegetal, do Departamento de Biologia Animal, do Departamento de Estatística e Investigação Operacional, do Departamento de Geologia, do Departamento de Matemática, do Departamento de Química e Bioquímica e do Departamento de Física

- 10.101.233.0/24

Rede das máquinas dos utilizadores pertencentes à CMU.

- 10.101.28.0/24, 10.101.32.0/24 e 10.101.36.0/24

Rede das máquinas do IBEB, do ICAT e do IO.

- 10.101.25.128/26

Rede das máquinas da Fundação da Faculdade de Ciências

Redes dos Alunos

Nesta secção são enumeradas todas as redes às quais os alunos de todos os departamentos de Ciências têm acesso.

- 10.101.124.0/24, 10.101.128.0/24, 10.101.132.0/24, 10.101.136.0/24, 10.101.144.0/24, 10.101.152.0/24, 10.101.156.0/24, 10.101.160.0/24, 10.101.163.0/24, 10.101.164.0/24, 10.101.165.0/24 e 10.101.167.0/24

Redes das máquinas das salas disponibilizadas aos alunos do Departamento de Engenharia Geográfica, Geofísica e Energia, do Departamento de Biologia Vegetal, do Departamento de Biologia Animal, do Departamento de Estatística e Investigação Operacional, do Departamento de Geologia, do Departamento de Matemática, do Departamento de Química e Bioquímica e do Departamento de Física. As quatro últimas redes correspondem a espaços abertos, como por exemplo, o espaço estudante.

- 10.101.168.0/24

Rede dedicada à associação de estudantes de Ciências.

- 10.101.169.0/24

Rede das tomadas de rede de acesso “livre”, isto é, onde os utilizadores podem ligar computadores portáteis sem autenticação prévia.

- 10.101.170.0/24

Rede usada para a realização de exames em laboratórios, que não tem acesso à rede externa, apenas ao moodle.

- 10.34.21.254/24

Rede dos laboratórios da Galp, que não pertence à gama 10.101 devido a um acordo que foi feito entre Ciências e a empresa Galp.

Redes de Voz

Nesta secção estão agrupadas todas as redes usadas por serviços de voz digital e analógico.

- 10.101.55.0/24

Rede dos telefones de VoIP da DSI

- 10.101.98.0/24

Rede para telefones VoIP, usada pelo Departamento de Física e pelo INETI.

- 10.101.180.0/24

Rede do PBX, usado pela central telefónica.

- 10.101.245.0/24

Rede do Servidor de VoIP (PBX)

Redes VPN

Grupo das redes VPN, para acesso à rede interna de Ciências.

- 10.101.104.0/24 e 10.101.166.0/24

Rede das VPN usadas, respetivamente, pelos docentes e alunos.

Redes de Serviços Públicos

Este grupo agrega os serviços públicos fornecidos por Ciências e redes para ligação externa.

• 194.117.42.0/28, 194.117.42.17/28, 194.117.42.33/28, 194.117.42.49/28, 194.117.42.97/27, 194.117.42.129/25, 194.117.44.0/24 e 194.117.45.0/28

Redes dos servidores públicos, especificamente do DNS, FTP, mail (2 gamas de endereços, MX e CAS), das aplicações, servidor web e do DI.

• 88.157.199.97/29

Rede de ligação à ZON, utilizada para ligação aos serviços da SIBS.

• 194.117.47.0/28 e 194.117.47.16/28

Rede de alojamento do servidor de VPN, e rede do Observatório astronómico onde está alojado o NTP.

Redes de Empresas

Aqui estão agrupadas as redes de empresas presentes na Organização.

• 10.101.33.0/24 e 194.117.49.0/27

Redes atribuídas às empresas alojadas no TecLabs. A primeira rede é privada e a segunda pública.

• 10.101.12.0/24

Rede das máquinas da associação de trabalhadores.

3.4 Melhorias de rede a implementar

Para estruturar a rede de Ciências de forma mais organizada, é sugerido que se diferenciem as redes existentes em três grupos: ensino, servidores e utilizadores. As redes de ensino incluem todas as redes de docentes, alunos, e laboratórios, sendo que todas têm uma máscara de 23bits, com algumas exceções, como é o caso da rede dos espaços estudante (21bits). A rede de servidores, inclui a rede do datacenter, atualmente alojada na gama 10.121.0.0/16, as redes públicas e de administração. Por fim, a rede dos utilizadores inclui todos os restantes grupos, as redes dos serviços académicos, associação de estudantes, etc.

Criando um domínio VTP para cada grupo, a rede passa a ser mais compartimentada e consequentemente, mais fácil de gerir. Adicionalmente, questões de sobrecarga de comutadores deixam de existir, pelo que é possível obter uma rede mais eficiente. É ainda importante referir que problemas que possam surgir dentro de um domínio VTP, não se irão propagar para outros domínios, logo a resolução de problemas torna-se menos complexa.

Capítulo 4

Administração de sistemas e segurança

4.1 Vulnerabilidades de serviços

Em 2015, o número de websites geridos pela DSI era de 325, onde 114 eram páginas pessoais de docentes. Os restantes incluem aqueles que geram mais tráfego, nomeadamente o portal de Ciências, webmail e moodle. A gestão de conteúdos de todos eles fica a cargo dos responsáveis e a gestão técnica a cargo do Núcleo de Infra-Estruturas de Serviços e Servidores.

4.2 Análise de vulnerabilidades

Da análise realizada, foi possível identificar servidores mal configurados e algumas falhas de segurança, ambos descritos e corrigidos mais à frente.

4.2.1 XSS no website de Ciências

Cross-Site Scripting, normalmente referido como XSS, é uma das falhas de segurança mais exploradas atualmente, ocupando a terceira posição no Top 10 da classificação da OWASP[3]. De forma muito resumida, este tipo de ataque explora a confiança que o navegador (do inglês *browser*) tem num determinado website vulnerável a XSS, permitindo a um utilizador malicioso executar código no navegador da vítima.

[3] https://www.owasp.org/index.php/Top_10_2013-Top_10

Antes de mais, note-se que este ataque apenas é possível se os dados manipulados pelo utilizador não forem verificados do lado do servidor. Apesar da verificação aparentar ser simples e óbvia, na verdade obriga à identificação de todos os campos onde serão manipulados dados pelo utilizador e exibidos pelo navegador algo que é frequentemente negligenciado pelo programador do servidor.

Embora não exista nenhuma classificação única de falhas XSS, é comum distingui-las entre persistentes e não persistentes, sendo que alguns especialistas consideram ainda um terceiro tipo, baseado em *DOM*.

Visto que o website de Ciências apenas está vulnerável a um destes tipos, o não persistente, apenas este será considerado.

O tipo de *Cross-Site Scripting* não persistente é o mais comum, sendo originado pela passagem direta dos dados inseridos pelo utilizador para os programas do lado do servidor sem que sejam devidamente tratados. Para executar tal ataque é usual recorrer a métodos de engenharia social, tais como induzir um utilizador a abrir uma mensagem de correio eletrónico falsa que contém um link para um website malicioso, e que ao ser carregado pelo navegador pode resultar em variadas consequências, que estão dependentes de vários fatores como o número de sessões ativas e válidas no sistema.

Daqui o utilizador malicioso pode obter credenciais da vítima ou realizar operações em nome desta.

A vulnerabilidade descrita foi encontrada no formulário de pesquisa do website principal de Ciências[4], apresentado na Figura 3 e após alguns testes foi confirmada a existência de tal vulnerabilidade. Mais tarde, acabou por se descobrir que esta vulnerabilidade estava presente em todos os formulários que aceitavam dados do utilizador. A seguir estão ilustrados os passos que possibilitaram a descoberta de tal problema:

Inserção de script aleatório que devolve o erro apresentado na Figura 4. Isto permitiu perceber que o servidor não fazia o tratamento dos dados inseridos pelo utilizador.

Seguidamente, através da observação da página HTML exibida no navegador foi localizado o código que originava o problema, utilizando um conjunto especial de carateres que facilitasse a deteção do problema ("*FINDXSS*"). Na Figura 5 é apresentado o código que permitia que a vulnerabilidade fosse explorada.

[4] ciencias.ulisboa.pt

Por fim, bastou escrever um pequeno script na linguagem Javascript que ilustrasse o problema. O script usado foi *"});});</script><script>alert('This website is vulnerable to XSS!')</script>*, que cria um simples *pop-up* com a mensagem *'This website is vulnerable to XSS!*. A Figura 6 confirma os resultados obtidos.

Figura 3: Campo de texto vulnerável

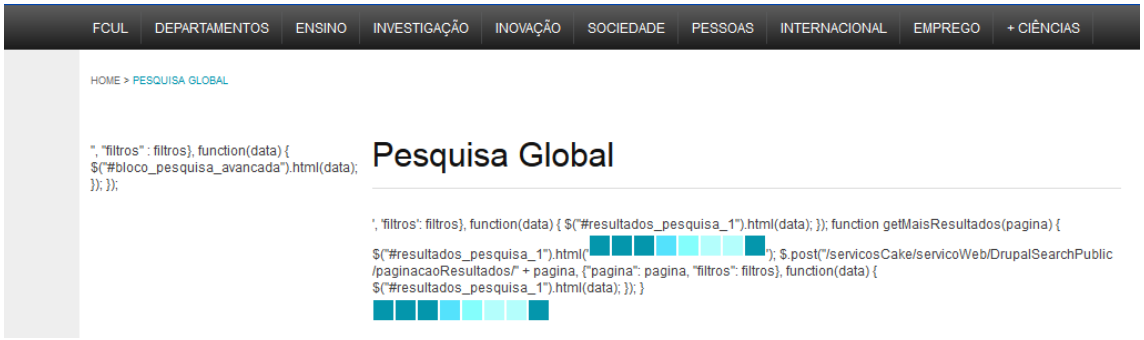


Figura 4: Erro apresentado quando o script é injetado

```
</script>
<script type="text/javascript">
var filtros = {"filtros_n":{"hidd":""},"contains":"FINDXSS","filtros_p":
                {"menu":"1","cursos":"1","disciplinas":"1","noticias":"1","eventos":"1",
                "videos":"1","paginas_depart_uni":"1","conferencias":"1"}};
$("#resultados_pesquisa_1").html(
            '<img src="/sites/all/themes/fcul/img/loader_horizontal.gif">');
$.post("/servicosCake/servicoWeb/DrupalSearchPublic/resultados",
            {"pesquisa" : ' FINDXSS', 'filtros': filtros}, function(data) {
$("#resultados_pesquisa_1").html(data);
});

function getMaisResultados(pagina) {
$("#resultados_pesquisa_1").html(
            '<img src="/sites/all/themes/fcul/img/loader_horizontal.gif">');
$.post("/servicosCake/servicoWeb/DrupalSearchPublic/paginacaoResultados/"
        + pagina, {"pagina": pagina, "filtros": filtros}, function(data) {
$("#resultados_pesquisa_1").html(data);
});
}
</script>
```

Figura 5: Código HTML que permite explorar vulnerabilidade

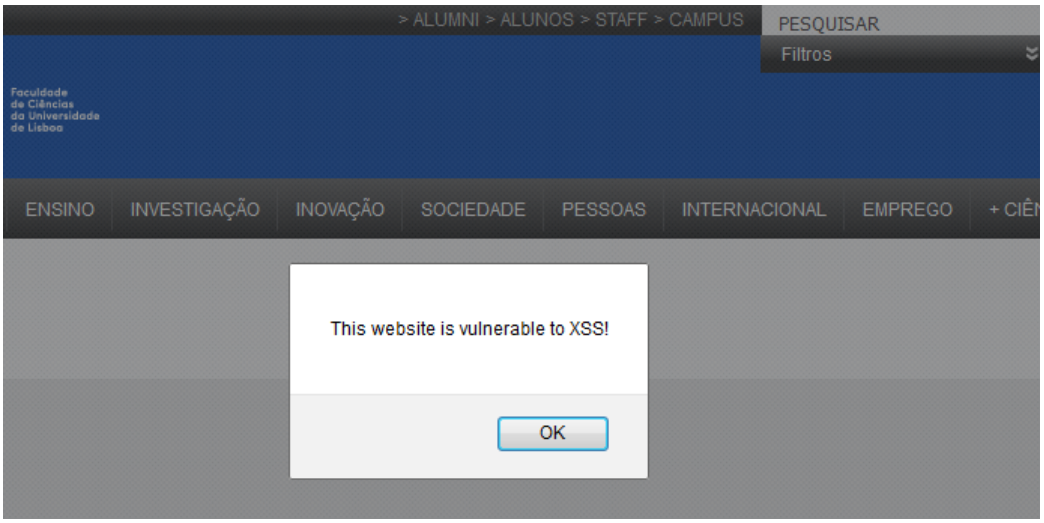


Figura 6: Resultados obtidos depois de explorar a vulnerabilidade

De forma a mitigar o problema a equipa de desenvolvimento da DSI optou por usar uma função PHP, *preg_replace*, usada para fazer o tratamento de dados passados pelo utilizador, garantindo que toda a pontuação é removida. Por fim, é importante referir que todas as alterações realizadas foram transparentes para o utilizador final e ainda que esta questão foi detetada na fase de transição de um website antigo para o novo, pelo que foi possível mitigar a vulnerabilidade antes do novo website de Ciências ficar ativo.

4.2.2 CSRF no website de Ciências

Cross-Site Request Forgery (CSRF) é também uma das falhas de segurança mais exploradas nos dias atuais, ocupando a oitava posição no Top 10 da OWASP. Resumidamente, este tipo de ataque envolve o envio de comandos não autorizados por

um utilizador legítimo para um website que confia no navegador desse utilizador. Tal como no XSS, para que o ataque seja bem sucedido, é necessário recorrer a métodos de engenharia social.

Note-se que tal vulnerabilidade existe devido ao facto de alguns websites realizarem certas operações com base num identificador submetido de forma automática, como por exemplo uma *cookie*.

Neste tipo de ataque, o utilizador é induzido a enviar pedidos maliciosos para um website, pelo que são necessários que estejam satisfeitos alguns requisitos:

O utilizador legítimo tem de estar autenticado no website vulnerável ao ataque, isto é, a sua sessão tem de estar válida.

O utilizador legítimo abre uma ligação do utilizador malicioso. É importante referir que esta hiperligação pode ser aberta através de variados métodos, onde os mais comuns são o envio de uma mensagem de correio eletrónico (engenharia social) ou a visita de uma página de um fórum que contém uma imagem com a hiperligação. É comum esta hiperligação conter um pedido HTTP. Para dificultar a deteção do ataque, o utilizador malicioso pode ofuscar o URL.

O navegador do utilizador legítimo envia o pedido malicioso para o servidor, usando a sua *cookie*[5].

É importante perceber que o website vulnerável não irá conseguir distinguir um pedido não autorizado de um legítimo, pois ambos vêm de um utilizador válido e com sessão válida. Este tipo de ataques visam, geralmente fazer alterações de dados pessoais ou mesmo movimentações financeiras, pelo que têm sempre como objectivo a realização de pedidos que resultem na alteração do estado do servidor.

Este problema foi identificado no website de Ciências usando a ferramenta de deteção de vulnerabilidades Acunetix[6].

Para mitigar o problema, existiam essencialmente duas soluções, o uso de *tokens* e a verificação do conteúdo do cabeçalho "*Referer*". A primeira solução é implementada no código de geração de *cookies* do lado do servidor, renovado periodicamente e que, por exemplo, pode ser incluído no URL das páginas do website. Basicamente, irá ser inserido um *nonce* em cada página com um formulário, de forma a garantir que não é

[5] Informação enviada por um website que é guardada pelo navegador de um utilizador

[6] https://www.acunetix.com/

submetido automaticamente. Algumas linguagens de programação já possuem bibliotecas para resolver esta questão. A segunda passa por perceber de que página o utilizador veio, isto é, comparar o campo *Referer* com o local onde o utilizador está a tentar aceder. Caso os domínios sejam diferentes, o acesso é bloqueado pois significa que o utilizador foi redirecionado de outra página, situação que é anómala. É ainda possível implementar ambas as soluções.

Existe ainda uma terceira solução, embora não aplicável a Ciências, que passa por exigir que o utilizador se autentique cada vez que realizar operações críticas.

Perante este problema e as soluções disponíveis, a equipa de desenvolvimento e de administração de sistemas da DSI optou por proceder à implementação dos *tokens*, o que eliminou o problema.

4.2.3 Vulnerabilidade Físicas

Ao nível de tomadas de rede disponibilizadas por Ciências, existem dois problemas. O primeiro é a clonagem do endereço de nível de ligação de dados, em que é alterado o MAC de uma placa de rede para poder ter acesso à rede. Isto porque as interfaces dos switches da organização estão configurados para enviar tráfego para MACs registados nas portas[7] do comutador, ou seja, descobrindo o MAC associado a uma tomada (algo que não é difícil), é possível cloná-lo e ter acesso à rede. Torna-se evidente que isto é uma ameaça à segurança da rede de Ciências, pois o utilizador (malicioso) adquire os privilégios do legítimo, podendo ter acesso a informação confidencial. O segundo problema consiste na ligação de equipamentos de rede, isto é, comutadores, encaminhadores (do inglês "router") ou APs, a tomadas de rede, algo que é proibido dentro da instituição. A DSI obriga os utilizadores a passarem por um processo de ativação de tomadas de rede, tendo estes que fornecer o seu nome e o endereço MAC da máquina que pretendem ligar a essa tomada (para associar à porta do comutador, como referido anteriormente). No entanto, alguns utilizadores não indicam o endereço MAC de uma máquina, mas sim de um equipamento de rede. É importante referir que esta questão pode ser parcialmente atribuída ao reduzido número de tomadas em algumas salas. Depois de este processo estar concluído, a informação do utilizador

[7] Estas portas estão também associadas a uma VLAN

que requisitou a tomada (Nome, endereço MAC, etc.) é guardada numa base de dados de administração. Esta página mantém também o estado (livre ou ocupada) de todas as tomadas de todos os comutadores da instituição, embora alguma informação esteja desatualizada, como por exemplo um comutador de 24 portas ter sido substituído no bastidor por um de 48 e na base de dados continuar o antigo.

Ainda em relação às tomadas de rede, a instituição garante que não existem tomadas de rede que permitam o acesso livre à rede interna/externa, à exceção de uma sala de reuniões, que embora esteja sempre trancada, tem tomadas de acesso livre para os utilizadores ligarem as suas máquinas pessoais apenas quando esta sala está a ser usada.

4.3 Ferramentas de Monitorização e Alarmística

Em relação a ferramentas de monitorização e alarmística, em Ciências é usado o OpManager[8], o Nagios[9] e o Observium[10].

A instituição tem uma licença para a edição "Essencial" da ferramenta de monitorização de rede OpManager, aplicada na monitorização de comutadores, UPSs, máquinas virtuais entre outras. Tal ferramenta está configurada para reportar, através de correio eletrónico, quando as taxas de utilização predefinidas pela equipa de administração de redes e sistemas são ultrapassadas. Esta é a ferramenta de monitorização e alarmística mais utilizada para gerir o parque informático de Ciências, tendo registados cerca de 475 dispositivos e 6500 interfaces. A Figura 7 apresenta uma imagem produzida por esta ferramenta.

[8] https://www.manageengine.com/network-monitoring/
[9] https://www.nagios.org/
[10] https://www.observium.org/

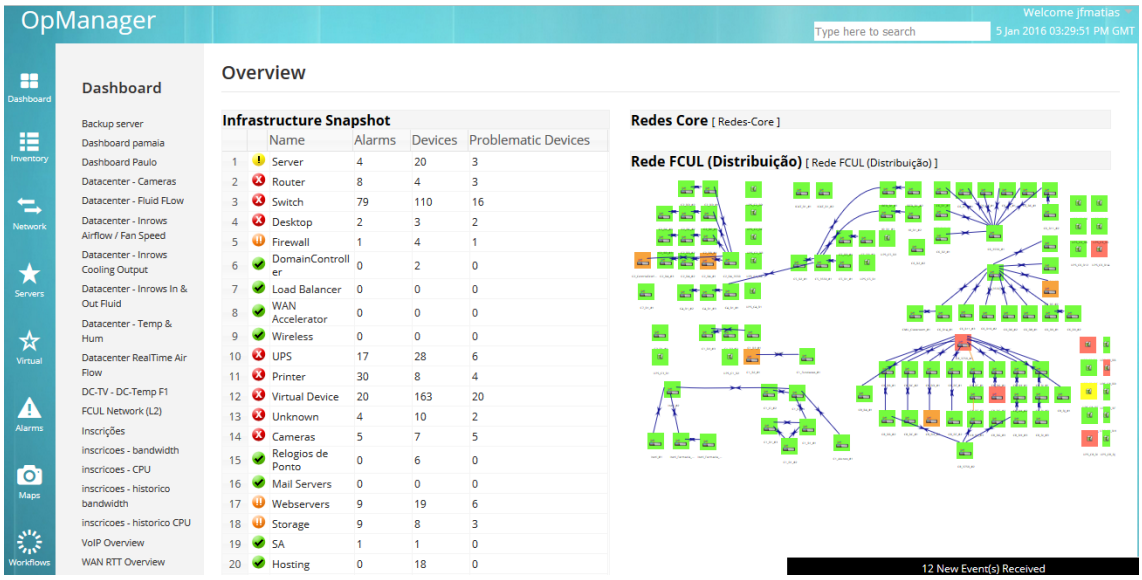


Figura 7: OpManager

Em relação à ferramenta Nagios Core, a instituição possui uma licença "Core DIY", responsável por monitorizar os 127 AP's de todo o campus e os servidores de alojamento. Os dados obtidos através desta ferramenta são depois interpretados (apenas para os AP's) por uma extensão, NagVis, através da disposição dos recursos monitorizados sobre um mapa, que no caso de Ciências, é o mapa do campus, permitindo saber a localização geográfica de uma dado AP. De referir que esta ferramenta é código aberto. A Figura 8 apresenta uma visão da consola do Nagios Core e a Figura 9 da extensão NagVis. A Figura 10 apresenta uma visão dos APs do edifício do C8.

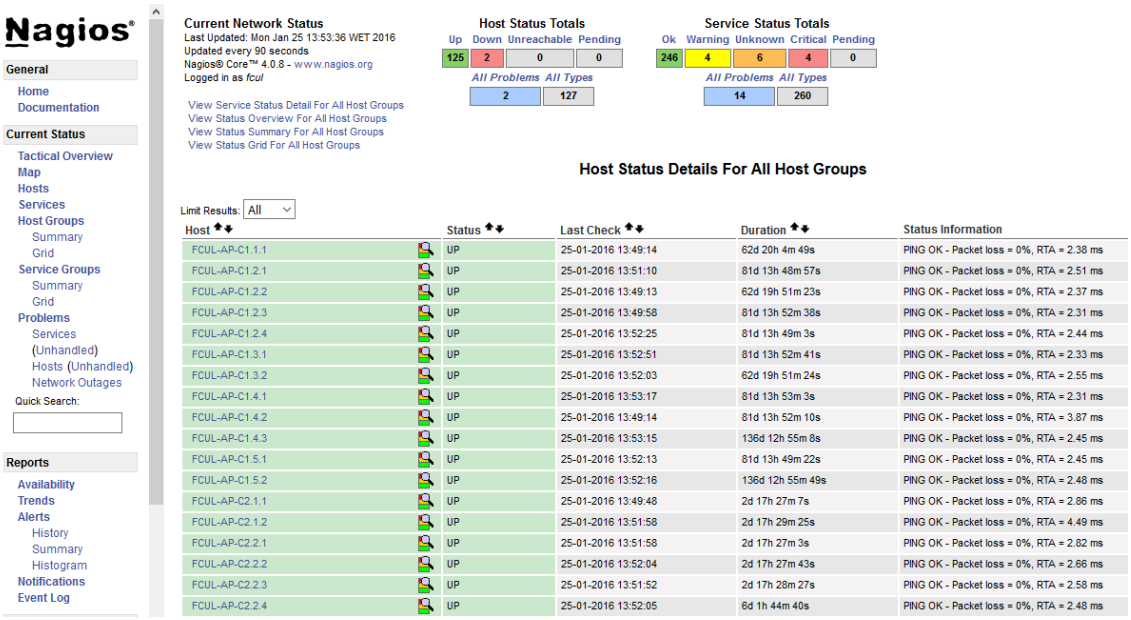


Figura 8: Nagios Core

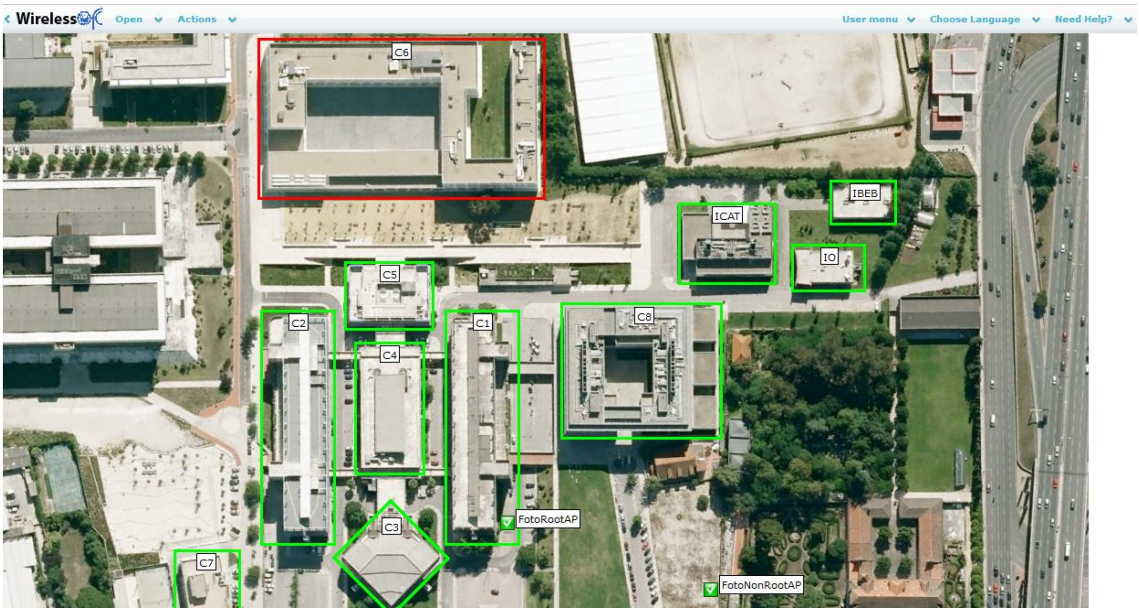


Figura 9: NagVis

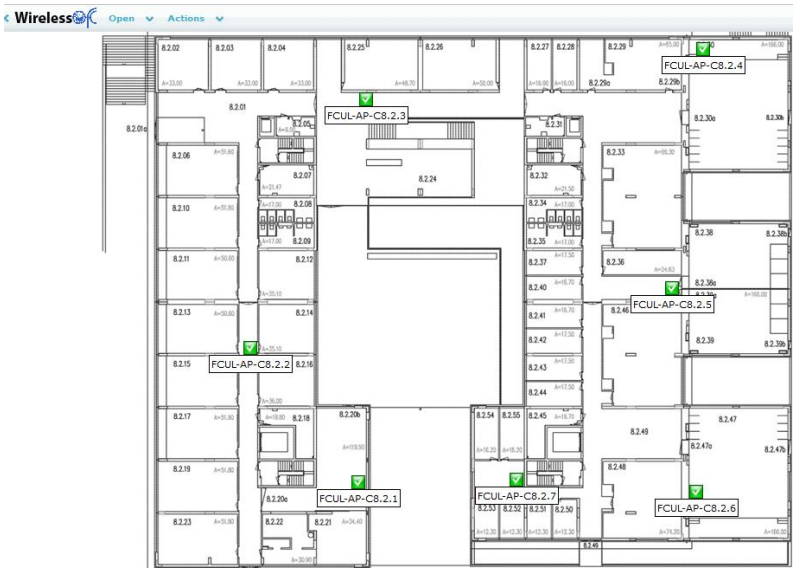


Figura 10: NagVis (Vista do edifício C8)

A última ferramenta é o Observium, para o qual existe uma licença da edição "Community", grátis, usada para monitorizar comutadores e firewall, assim como as respetivas interfaces (cerca de 6500) e ainda todo o hardware de armazenamento. Esta ferramenta é também utilizada para monitorizar a utilização da VPN. A Figura 11 apresenta esta ferramenta.

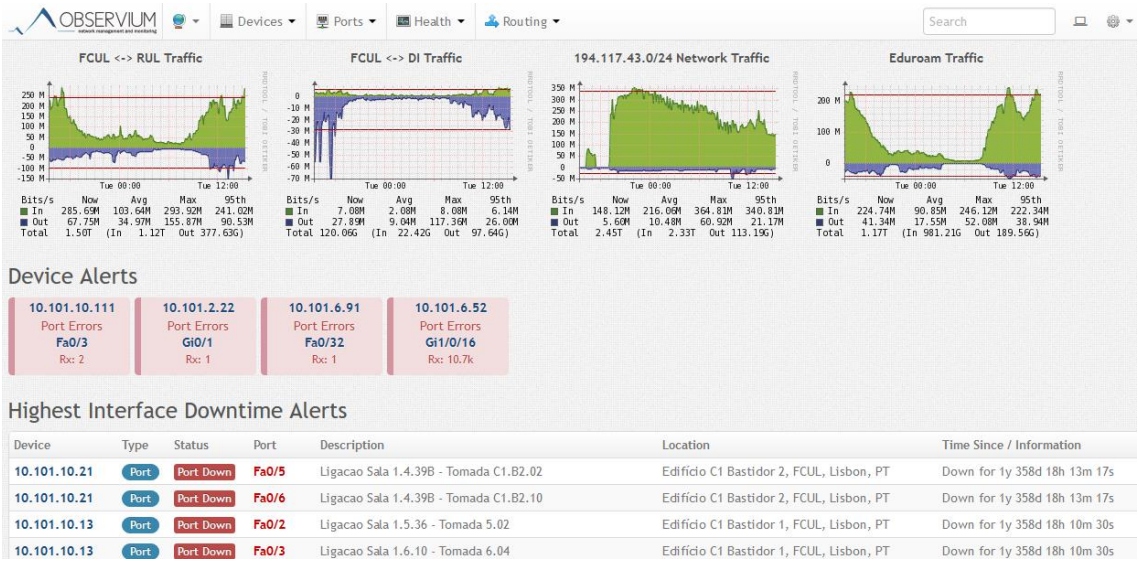


Figura 11: Observium

Por fim, e depois de todas as ferramentas de monitorização terem sido apresentadas, é possível perceber que a monitorização da rede é também um problema, pois é feita através de três ferramentas, o que não é ideal para a descoberta e procura de informação nem para a realização de atividades de diagnóstico uma vez que a informação está demasiado dispersa pelas três plataformas, cada uma a operar de forma diferente e a produzir alertas para o correio eletrónico dos gestores. Isto torna-se confuso, pelo que seria ideal agrupar a monitorização de todo o hardware da instituição numa única ferramenta.

4.4 AAA em Ciências

Em Ciências, para identificar utilizadores, permitir a realização de certas operações e para perceber que tipo de recursos utilizam durante o acesso, são utilizados protocolos de Authentication, Authorization, and Accounting (AAA), nomeadamente o RADIUS e TACACS.

Um servidor RADIUS autentica utilizadores para acesso remoto, protegendo a rede contra acessos não autorizados. Este servidor é ainda usado pelo serviço de VPN e 802.1x[11].

[11] 802.1X é um standard da IEEE para controlo de acesso à rede através de credenciais. É usado para dar rede a portáteis de utilizadores, atribuindo a rede a que têm acesso.

Existe também um servidor TACACS com o protocolo TACACS+ implementado, para autorizar acessos de utilizadores da DSI aos comutadores de rede, sendo que esses acessos ficam no log deste servidor.

Por fim, existe um servidor NPS, que não é mais do que um RADIUS mas implementado pela Microsoft. Atualmente é também usado para controlo de acesso à rede através de 802.1x.

4.5 SSL em Ciências

4.5.1 Websites

O SSL e o TLS são protocolos criptográficos que fornecem segurança à comunicação, fornecendo privacidade e integridade de dados ponto a ponto. Por estar implementado nos websites de Ciências, é garantido que informação sensível, tais como credencias de acesso, é transmitida de forma segura.

Do levantamento feito, foi possível inferir que os seguintes websites da instituição têm SSL implementado:

- id.fc.ul.pt
- ciencias.ulisboa.pt
- webmail.ciencias.ulisboa.pt
- suporte.ciencias.ulisboa.pt
- webpages.ciencias.ulisboa.pt
- chairs.campus.ciencias.ulisboa.pt
- www.micobiotas.fc.ul.pt
- fenix.ciencias.ulisboa.pt

Para estes, e usando a ferramenta SSLLABS[12] para analisar a configuração do SSL nos servidores de Ciências, foi possível identificar algumas configurações incorretas. Destas destacam-se a escolha de algoritmos criptográficos feita pelo cliente e não pelo servidor web e o uso de alguns algoritmos criptográficos desatualizados como é o caso do RC4. Depois de uma análise detalhada, e tendo em conta vários fatores, como por

[12] https://www.ssllabs.com/ssltest/index.html

exemplo o tipo de utilizadores que fazem acessos aos websites referidos, eis as alterações que foram feitas, em servidores com NGINX e Apache:

A seleção do algoritmo criptográfico passa a ser feita pelo servidor. Para isto, o servidor analisa a lista de algoritmos que o cliente suporta escolhendo o mais adequado de acordo com a sua própria lista organizada por ordem de preferência.

Algoritmos fracos como MD5 e RC4 deixam de ser usadas. Deixa também de ser permitida a comunicação sem autenticação ou mesmo sem o uso de cifra.

Os parâmetros Diffie-Hellman passam a ter no mínimo 2048 bits, e não 1024 como estava previamente definido. No entanto, não foi possível efetuar tal alteração em servidores Apache devido à versão em uso.

Foi implementado o mecanismo HSTS, que previne ataques que visam usar algoritmos fracos e desatualizados quando estão disponíveis algoritmos robustos. A comunicação passa também a ser feita apenas através de HTTPS, pois todos os pedidos HTTP são redirecionados para HTTPS.

Foi implementada a configuração *OCSP stapling*, que transfere o processo de verificação do estado de um certificado, isto é, se foi revogado ou está válido, para o servidor. Esta operação é normalmente realizada pelo navegador do cliente, o que levanta questões de privacidade, pois a entidade certificadora consegue identificar o website a que um utilizador específico tentou aceder. Existe ainda o problema do tempo adicional que o cliente demora a obter a resposta da entidade certificadora, que pode ser ampliado pela carga excessiva dos servidores dessa entidade. Com esta configuração todos estes problemas são resolvidos pois o servidor que o utilizador visita, mantém em *cache* a resposta do servidor OCSP.

A lista de algoritmos que os servidores de Ciências suportam, incluindo algoritmos amplamente difundidos de forma a suportar clientes mais antigos, passou a ser:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES128-GCM-SHA256

- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- ECDHE-RSA-DES-CBC3-SHA
- DES-CBC3-SHA

A implementação de todas as configurações descritas anteriormente ficou a cargo da equipa de administração de sistemas da DSI.

Na Figura 12 são apresentados resultados obtidos pela ferramenta referida.

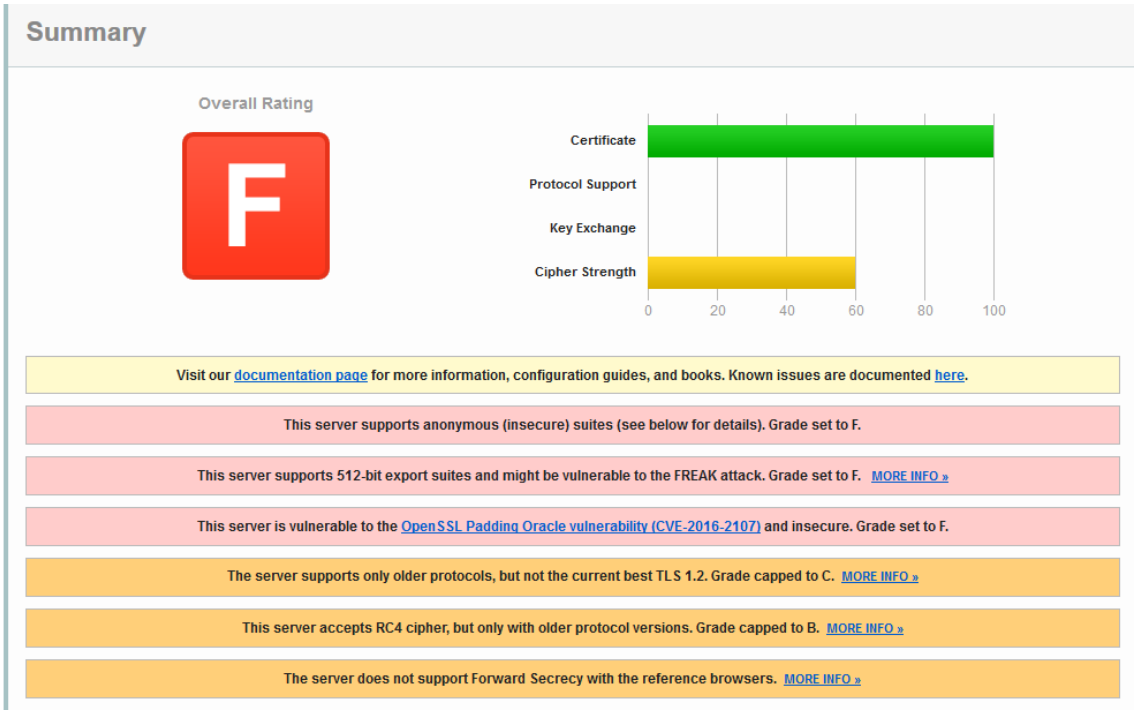


Figura 12: Resultado para id.fc.ul.pt

4.5.2 Correio Eletrónico

Ciências faz uso de três protocolos de correio eletrónico POP3, IMAP e SMTP. Para garantir que toda a informação relacionada com os utilizadores, tal como as

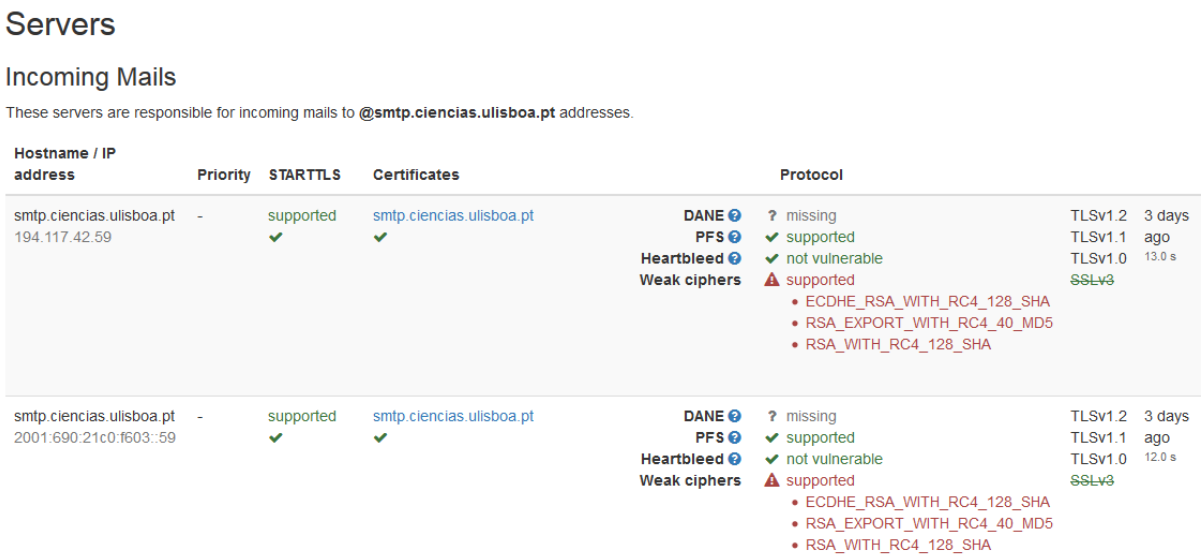
credencias, é enviada através de uma ligação segura os servidores de correio eletrónico suportam SSL. Os serviços para os quais o SSL está implementado são:

- smtp.ciencias.ulisboa.pt
- imap.ciencias.ulisboa.pt
- pop.ciencias.ulisboa.pt

Dos três, o SMTP é o que exige mais atenção às configurações. Dos níveis de segurança disponibilizados pelo Postfix, foi adotado o oportunista (do inglês o*pportunistic*), através da configuração *smtp_tls_security_level = may*, isto porque com o nível de segurança seguinte, se ocorrer algum tipo de erro durante o envio da mensagem de correio eletrónico, como por exemplo o cliente não suportar SSL, a mensagem não será enviada. Ao usar o nível de segurança escolhido, se a ligação SSL falhar tenta-se estabelecer a ligação novamente, mas sem usar SSL. Esta solução é a mais adequada tendo em conta que na instituição existem máquinas bastante antigas e que muito provavelmente não suportam SSL.

Foram feitas mais configurações como a escolha dos protocolos a utilizar e, mais importante, foram implementadas soluções para reduzir mensagens de *spam*.

Na Figura 13 são apresentados resultados obtidos por uma ferramenta para testar configurações de servidores de correio eletrónico.



Servers

Incoming Mails

These servers are responsible for incoming mails to **@smtp.ciencias.ulisboa.pt** addresses.

Hostname / IP address	Priority	STARTTLS	Certificates	Protocol			
smtp.ciencias.ulisboa.pt 194.117.42.59	-	supported ✔	smtp.ciencias.ulisboa.pt ✔	DANE PFS Heartbleed Weak ciphers	? missing ✔ supported ✔ not vulnerable ⚠ supported • ECDHE_RSA_WITH_RC4_128_SHA • RSA_EXPORT_WITH_RC4_40_MD5 • RSA_WITH_RC4_128_SHA	TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	3 days ago 13.0 s
smtp.ciencias.ulisboa.pt 2001:690:21c0:f603::59	-	supported ✔	smtp.ciencias.ulisboa.pt ✔	DANE PFS Heartbleed Weak ciphers	? missing ✔ supported ✔ not vulnerable ⚠ supported • ECDHE_RSA_WITH_RC4_128_SHA • RSA_EXPORT_WITH_RC4_40_MD5 • RSA_WITH_RC4_128_SHA	TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	3 days ago 12.0 s

Figura 13: Resultados para smtp.ciencias.ulisboa.pt

Capítulo 5
Regulamentação e formalização de procedimentos

Da avaliação da infraestrutura da instituição, foi possível perceber que não existia nenhum documento que fizesse a listagem de políticas ou mesmo procedimentos de segurança. As políticas fornecem orientações aos indivíduos dentro de uma organização sobre o comportamento esperado, sendo estas políticas explícitas e concisas, expondo de forma clara os métodos que a organização pretende pôr em prática de forma a proteger os ativos que são de sua responsabilidade. Por outro lado, os procedimentos de segurança são um conjunto de instruções detalhadas que um indivíduo deve seguir de forma a conseguir implementar as políticas de segurança. Todos os documentos mencionados são apresentados no anexo B.

Posto isto, foram redigidos ambos os documentos. A estrutura das Políticas de Segurança de Informação começa por atribuir responsabilidades às diferentes equipas da DSI de Ciências, define sanções a serem aplicadas em caso de incumprimento, a vida útil do documento, informações de contactos e por fim as políticas. As políticas implementadas foram:

- Política de BYOD

Ciências é uma instituição com cerca de 5500 utilizadores, com liberdade para ligarem qualquer um dos seus vários dispositivos à rede. Isto permite à instituição reduzir custos relativamente à aquisição, manutenção e gestão de máquinas, pois os dispositivos passam a ser os dos utilizadores. No entanto, obriga à definição de uma política que estabeleça regras de utilização.

- Política de Classificação de Informação

Ciências, tal como muitas outras instituições possui informação mais crítica que outra, daí surgir a necessidade de criar uma política que facilite a atribuição de níveis de classificação a diferentes tipos de informação.

- Política de Controlo de Acesso

A instituição possui uma rede de média dimensão e fisicamente disponível a qualquer pessoa. Daqui vem a necessidade de implementar medidas para controlo de

acesso nos sistemas informáticos de Ciências. Existe também a necessidade de lidar com os diferentes tipos de utilizadores da instituição e com as permissões de acesso associadas a cada um deles.

- Política de Desenvolvimento Seguro

Por serem desenvolvidos programas internamente, justifica-se a existências desta política, pois é importante que a informação seja manuseada de forma apropriada.

- Política de Destruição

Toda a informação pertencente a Ciências, quer seja física ou digital, que já não tenha valor tem que ser destruída de acordo com certas regras para que dados sensíveis não sejam expostos. Esta política define quem é responsável por realizar tal processo e os meios que são permitidos utilizar.

- Política de Dispositivos Móveis e Teletrabalho

Na era atual, é muito comum utilizadores trabalharem a partir de casa, o que do ponto de vista de segurança informática representa um grande risco para as instituições pois não é possível controlar as máquinas usadas para aceder à rede. Posto isto, é necessário uma política desenhada de acordo com as necessidades específicas desta instituição para que toda a informação contida em máquinas que saem do campus de Ciências esteja segura, e ainda que clarifique como é feito o acesso à rede interna a partir do exterior.

- Política de Gestão de Desastres

É necessária uma política que identifique os documentos para gestão de desastres que a instituição precisa de elaborar, e que explique como tais documentos devem ser estruturados e o objetivo de cada um. A necessidade de tal política advém do facto de qualquer instituição estar sujeita, por exemplo a desastres naturais, e ainda da necessidade de rápida recuperação nessa eventualidade.

- Política de Gestão de Incidentes de Segurança

Qualquer instituição com presença na rede pública está sujeita a ataques, pelo torna-se inevitável a existência desta política, capaz de enumerar as entidades a quem

recorrer e a melhor forma de lhes responder, por forma a assegurar a integridade, confidencialidade e disponibilidade dos dados.

- Política de Palavra Passe

As credenciais de acesso aos recursos da instituição são o nome de utilizador e a palavra passe associada. Estas credenciais impedem o acesso não autorizado às plataformas informáticas de Ciências. Visto que o nome de utilizador é público, resta garantir a máxima robustez possível da palavra passe, impondo aos utilizadores regras mínimas para a sua criação.

- Política de Salvaguarda de Informação

A existência de tantos utilizadores com informação alojada em Ciências obriga a uma disponibilidade imediata dos dados, para que em situação adversa não sejam perdidos. Daqui surge a necessidade da criação de cópias de segurança, pelo que esta política vem especificar como tal processo é efetuado.

- Política de Proteção Individual dos Dados

Com a existência de máquinas acedidas por um grande número de utilizadores, torna-se fulcral desenvolver regras básicas para proteger a informação pessoal de tais utilizadores e para evitar questões de roubo de credenciais ou mesmo de sessões.

- Política de Gestão de Chaves Criptográficas

Por manipular informação pessoal dos utilizadores, torna-se evidente que a instituição precisa de ter métodos implementados para cifrar dados, independentemente de serem transmitidos para a rede exterior. É então criada a necessidade da existência de uma política que garanta que as chaves utilizadas para esta finalidade estão seguras, fornecendo orientações para atingir tal objetivo.

- Política de Transferência e Armazenamento Pessoal de Informação

Por fornecer métodos para a transferência e armazenamento pessoal de informação, é necessário que Ciências possua um conjunto de critérios que clarifiquem as operações permitidas para os diferentes serviços da instituição.

Resta mencionar que até à data estas foram as únicas políticas redigidas, pois são aquelas que se aplicam à instituição, o que não significa que mais tarde, com a evolução da infraestrutura física e tecnológica de Ciências não possam ser adicionadas mais políticas. As políticas descritas devem também ser atualizadas frequentemente.

O documento Procedimentos de Segurança inclui também as informações de contactos e os seguintes procedimento:

- Procedimento para Acesso à Rede Física
- Procedimento para Alteração de Palavra Passe
- Procedimento para Gestão de Incidentes
- Procedimento para Definição de Valor da Informação
- Procedimento para Destruição de Informação
- Procedimento para Realização de Cópia de Segurança
- Procedimento para Criar e Eliminar Utilizadores
- Procedimento para Teletrabalho
- Procedimento de Testes de Eletricidade
- Procedimento de Testes de Backup

Estes procedimentos são requisitos de algumas políticas de segurança.

Ambos os documentos foram revistos e aprovados pelo atual coordenador da Direção de Serviços Informáticos.

Depois destes documentos, foi ainda criado o Plano de Contingência, documento com o objetivo de ajudar uma organização a responder de forma eficaz a adversidades que possam ou não surgir. Perante isto, tal plano foi desenvolvido de acordo com as necessidades de Ciências, no qual foram descritos vários cenários, constituídos por serviços alvo e diversos eventos associados. O plano implementado inclui os cenários:

- Incêndio e acesso não autorizado ao Datacenter
- Escassez de recursos e comprometimento do anfitrião relativamente ao software de virtualização
- Defacement e SQL Injection nos websites aos quais a instituição fornece alojamento

Os cenários enumerados, têm em consideração situações possíveis de ocorrer na instituição. Este documento deve ser atualizado com base em eventos realizados com o

intuito de testar a capacidade de instituições responderem a determinadas situações adversas, como é o caso do CIBER PERSEU[13].

Todos os documentos referidos têm que ser regularmente revistos e atualizados.

[13] Exercício realizado pelo exército português, com o objetivo exercitar e avaliar a capacidade de respostam relativamente à ocorrência de ciberataques, de âmbito nacional ou internacional.

Capítulo 6

Conclusões

Durante os últimos meses tive a oportunidade de compreender melhor como funciona a infraestrutura tecnológica de Ciências, e identificar os problemas existentes. Daqui, tive ainda a oportunidade de sugerir possíveis resoluções para tais problemas. Como trabalho futuro, aponta-se a necessidade de melhorar o plano de contingência, com a introdução de novos cenários e a melhoria dos documentos políticas e procedimentos de segurança, com base na revisão destes documentos pelos vários elementos da DSI.

Acrónimos

AAA – Autenticação, Autorização e Auditoria

AP – Access Point

CAS - Central Authentication Service

DI – Departamento de Informática

DNS - Domain Name System

DSI – Direção de Serviços Informáticos

FCUL – Faculdade de Ciências da Universidade de Lisboa

FTP - File Transfer Protocol

IBEB – Instituto de Biofísica e Engenharia Biomédica

ICAT – Instituto de Ciência Aplicada e Tecnologia

IDP - Intrusion Detection and Prevention

INESC - INstituto de Engenharia de Sistemas e Computadores

INETI - Instituto Nacional de Engenharia, Tecnologia e Inovação

IO – Instituto de Oceanografia

MAC - Media Access Control

MPPS – Million Pakets per Second

MX - Mail Exchanger

NAS - Network-Attached Storage

NAT – Network Address Translation

NPS – Network Policy Server

NTP - Network Time Protocol

PAT – Port Address Translation

PVST+ – Per-VLAN Spanning Tree Plus

RADIUS - Remote Authentication Dial-In User Service

SSH - Secure Socket Shell

STP - Spanning Tree Protocol

TACACS – Terminal Access Controller Access Control System

ULisboa – Universidade de Lisboa

UPS - Uninterruptible Power Supply

UTL – Universidade Técnica de Lisboa

VLAN – Virtual Local Area Network

VoIP - Voice over Internet Protocol

VPN – Virtual Private Network

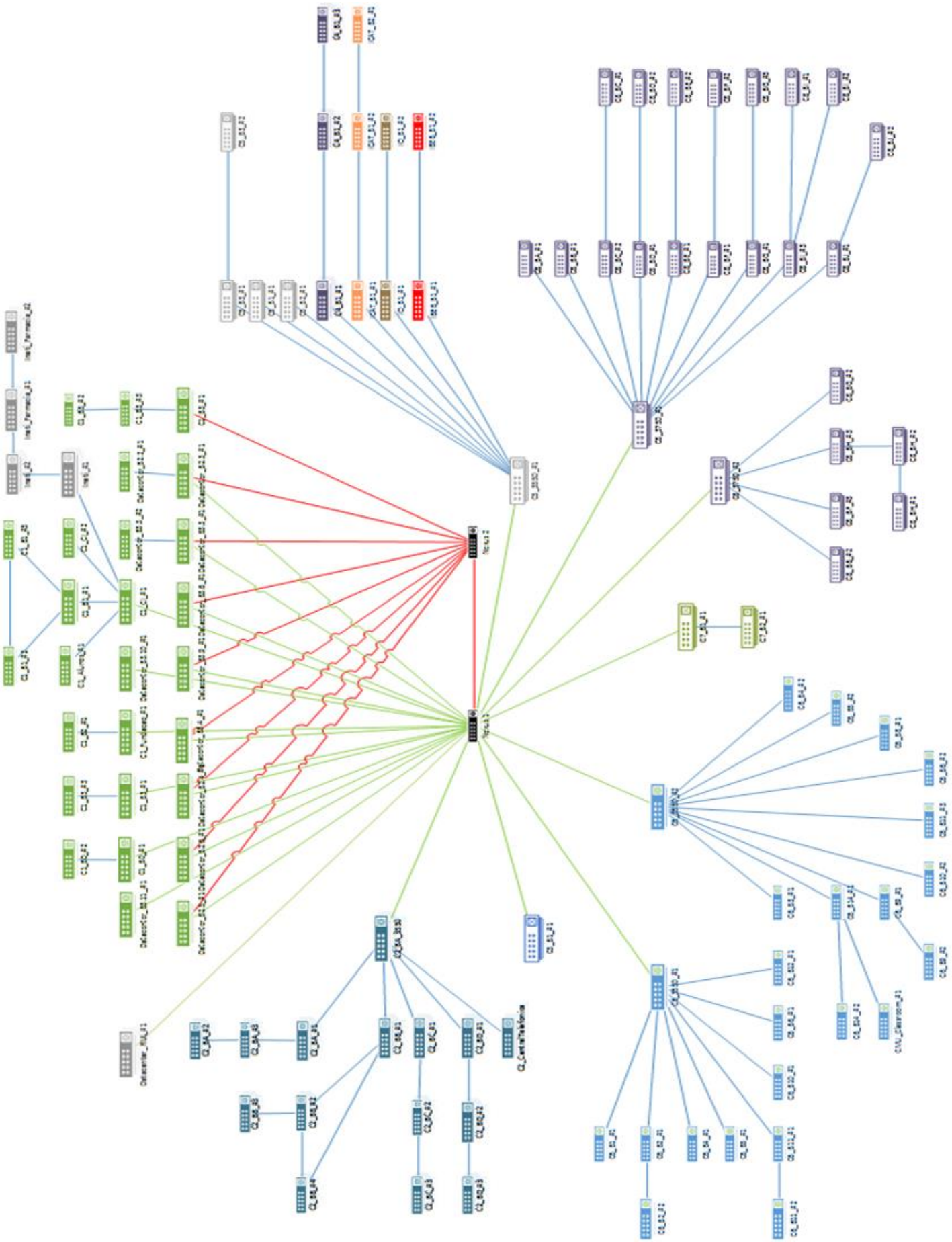
VTP - VLAN Trunking Protocol

Bibliografia

Saltzer, J. & Schroeder, M. (1975). The protection of information in computer systems. Proceedings of the IEEE. 63 (9), 1278-1308. doi:10.1109/PROC.1975.9939

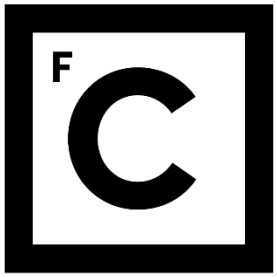
Anexos

Anexo A – Mapa de Rede Nível 2



Anexo B – Documentos Internos

POLÍTICAS DE SEGURANÇA DE INFORMAÇÃO



Ciências
ULisboa

Faculdade
de Ciências
da Universidade
de Lisboa

Classificação:	Público
Código do Documento:	PSI_DSI
Versão do Documento:	1.2
Data da Última Revisão:	26 de Setembro de 2016
Elaborado por:	Direção de Serviços Informáticos
Verificado por:	Coordenador da Direção de Serviços Informáticos

Índice

Informação Gerais

Direção de Serviços Informáticos de Ciências

DIREÇÃO DE SERVIÇOS INFORMÁTICOS

Faculdade de Ciências da Universidade de Lisboa

Edifício C1, Piso 2, Sala 1.2.10

Campo Grande 1749-016

Lisboa

Telefone Geral:	217 500 000
Extensão Interna:	21248
Correio Eletrónico:	suporte@ciencias.ulisboa.pt
Horário Atendimento:	08H00 – 18H00 (2ª, 4ª, 5ª e 6ª feira)
	08H00 – 19H00 (3ª feira)

CERT.PT

Correio Eletrónico:	cert@cert.pt
Telefone Geral:	210497399

A Política de Segurança de Informação é um documento dinâmico pois é necessário ser atualizado sempre que sejam efetuadas alterações que afetem as presentes políticas. Fica a cargo da DSI rever e atualizar este documento sempre que necessário, com uma frequência necessariamente inferior a um ano.

Introdução

A Faculdade de Ciências da Universidade de Lisboa é uma instituição de ensino universitário público, que centra a sua atividade no ensino e na investigação científica, e que alberga diferentes departamentos e unidades de serviço distribuídos pelo campus. A nível de tecnologias de informação e comunicação, Ciências possui um conjunto de sistemas de informação suportados por uma rede cablada e por uma rede sem fios.

Esta instituição tem na sua posse informação sobre os seus utentes, incluindo informação bancária e dados pessoais, o que obriga a um manuseamento prudente e à manutenção de uma infraestrutura tecnológica cuidada.

Qualquer serviço fornecido através de sistemas informáticos tem um fator de insegurança associado, nomeadamente vulnerabilidades, pelo que Ciências não é exceção. É então necessário desenvolver estratégias para proteger de forma adequada a informação retida por esta instituição.

As políticas de segurança de informação são um conjunto específico de requisitos e regras que precisam de ser satisfeitas de forma a garantir a segurança e privacidade dos dados de uma organização. Este documento define um conjunto de políticas que se consideram adequadas para os tipos de dados e necessidades da Faculdade de Ciências da Universidade de Lisboa, aproximando-a das políticas impostas pela norma ISO 27001 e que são globalmente reconhecidas como boas práticas de gestão de sistemas de informação.

Objetivos

As políticas de segurança da informação visam proteger todos os ativos de informação, definindo um conjunto de diretivas para garantir as seguintes propriedades relativamente aos sistemas e tecnologias da informação:

Confidencialidade – garante que a informação não está disponível ou que não é revelada a indivíduos não autorizados, entidades ou processos

Integridade – garante que a informação não é modificada ou destruída por indivíduos não autorizados, entidades ou processos, salvaguardando a fiabilidade e origem

Disponibilidade – garante que a informação está acessível e utilizável por indivíduos autorizados, entidades ou processos

Espera-se que num futuro próximo, este documento conduza à aplicação de práticas mais seguras na interação com sistemas de informação.

Pretende-se ainda que este documento identifique e atribua responsabilidades relativamente à gestão de informação e ao respeito pelas propriedades acima mencionadas.

O presente documento considera que a entidade responsável pela Política de Segurança da Informação é a Direção de Serviços Informáticos de Ciências.

Âmbito

A presente política aplica-se à Faculdade de Ciências da Universidade de Lisboa, o que inclui todos os departamentos, unidades de serviços, colaboradores e alunos que tenham acesso aos sistemas de informação da instituição. Torna-se assim indispensável assegurar que todos os utentes da instituição tenham conhecimento desta política.

Responsabilidades

Direção de Serviços Informáticos

As responsabilidades atribuídas ao gabinete e áreas que constituem a DSI estão estabelecidas no Despacho n.º 9353/2016, de 21 de julho.
Consideram-se como utilizadores os alunos, docentes, investigadores, bolseiros, funcionários e utilizadores com ligação temporária a Ciências.
Os utilizadores partilham com a DSI a responsabilidade por:

- Proteger a sua informação de autenticação
- Salvaguardar a sua informação pessoal
- Preservar os equipamentos informáticos fornecidos por Ciências, que se destinam exclusivamente à atividade de ensino e investigação
- Cumprir os termos e condições de utilização de qualquer software disponibilizado pela instituição
- Não divulgar informação de acesso restrito que lhe seja confiada

Para além de eventuais procedimentos que resultem da violação intencional e deliberada desta política por parte de um utilizador, qualquer violação terá como sanção o bloqueio da conta de utilizador até que a situação se considere regularizada.

Recebendo a DSI a notificação da cessação da relação entre um utilizador e a instituição é sua responsabilidade revogar todos os seus acessos físicos e lógicos aos sistemas informáticos respeitando as normas definidas, e ainda proceder à salvaguarda dos dados não pessoais para posteriormente serem disponibilizados às entidades responsáveis.

No âmbito das suas funções, cabe à DSI a gestão de segurança da informação e a salvaguarda dos dados recolhidos e produzidos pela instituição. Esta equipa é também responsável por aproximar as políticas de segurança de informação da instituição de padrões reconhecidos internacionalmente, como é o caso da norma ISO 27001, e por validar as especificações dos projetos de alterações em matéria de segurança.
Adicionalmente tem a responsabilidade de manter os documentos de Políticas de Segurança, Procedimentos de Segurança e Plano de Contingência atualizados.

Compete à gestão de topo da Direção de serviços informáticos aprovar documentos internos e assegurar que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a orientação estratégica da organização. Compete ainda garantir que o presente documento está disponível aos utentes de Ciências e que estes têm conhecimento das políticas existentes.

Políticas

Política de BYOD

Ciências permite que todos os seus utentes usem os seus dispositivos pessoais dentro da instituição, assegurando a conectividade à Internet através de rede sem fios *eduroam*. Esta rede obriga à autenticação dos utilizadores com as suas credenciais. Ciências permite ainda que utilizadores autenticados tenham acesso à rede cablada, mediante um pedido de ativação de tomada de rede feito à DSI.

Não é permitida a utilização dos equipamentos informáticos ou a conectividade à rede de Ciências para produção, alojamento e/ou distribuição de conteúdos com objetivos comerciais, partidários, religiosos, racistas, obscenos, pornográficos ou outros que sejam contraditórios com a missão da instituição.

Os utentes assumem total responsabilidade pelos riscos, incluindo a perda de dados ou algum tipo de falha que torne o dispositivo inutilizável, assim como por quaisquer tipos de danos que software instalado nos seus dispositivos pessoais possam provocar nos sistemas informáticos de Ciências.

Política de Classificação de Informação

A informação física e digital pertencente à Faculdade de Ciências da Universidade de Lisboa tem um grau de classificação de segurança associado, baseado no valor da informação, importância, sensibilidade em caso de divulgação ou modificação não autorizada.

Define-se que os graus de classificação de segurança da informação em vigor são os seguintes:

Confidencial

Informação sensível para a instituição, acessível a grupos específicos de utilizadores, e cuja divulgação pública acarreta danos para a instituição ou para os utilizadores. Este tipo de informação deve ser acedido apenas pelos utentes diretamente envolvidos no seu manuseamento.

Interna

Informação disponível apenas a utilizadores de Ciências, a qual é protegida do acesso exterior através de autenticação. O acesso não autorizado a informação assim classificada pode resultar em danos limitados para a instituição.

Pública

Informação disponível a qualquer entidade exterior a Ciências.

Política de Contas

As contas de utilizador são necessariamente associadas ao nome completo e ao número do documento de identificação de um utente de Ciências. A associação pode ser direta ou indireta, nos casos em que a conta é criada para suportar um utilizador ou atividade temporária. Estas contas podem ser de dois tipos:

Contas de Utilizadores de Ciências

Ciências define contas de aluno, docente, investigador, bolseiro e funcionário de acordo com a relação que cada utilizador mantém com a instituição.

Contas de Utilizadores com ligação temporária a Ciências.

As contas de utilizadores com ligação temporária à instituição, subdividem-se em dois tipos, contas "Convidado" e contas "Conferência". A conta de conferência pode ser partilhada por um grupo de utilizadores. A conta de visitante é obrigatoriamente individual. Ambas são criadas quando solicitado por estes utilizadores e são aprovadas pela DSI, tendo obrigatoriamente um tempo limite para expirar. Tais contas permitem o acesso à rede sem fios.

Política de Controlo de Acesso

Ciências implementa um sistema de gestão de identidade de utentes, sem exceções, onde são definidos os diferentes níveis de acesso consoante o tipo de conta. O controlo de acesso é aplicado a todos os sistemas e serviços da instituição, de forma a fornecer, não só o nível de acesso atribuído ao utilizador, mas também para preservar a confidencialidade, integridade e disponibilidade dos dados mantidos em Ciências de acordo com a classificação de segurança da informação. Sem prejuízo de mecanismos mais fortes que venham a ser definidos, todos os utilizadores são autenticados por um par nome de utilizador/palavra passe. Não é permitida a partilha destas credenciais de acesso, excetuando o caso das contas temporárias do tipo Conferência.

O acesso à infraestrutura física e aos Sistemas de Informação de Ciências é restrito a utentes autorizados e autenticados, com a exceção de websites de divulgação de conteúdos públicos, pelo que as configurações de segurança de tais sistemas devem ser adaptadas a esta política.

Não deverá ser possível qualquer acesso anónimo aos SI, pelo que contas do tipo "Convidado" não devem existir em nenhuma máquina da instituição.

A instituição deve dar acesso limitado aos fornecedores para acederem tanto à infraestrutura como à informação, pelo que não devem ter mais permissões do que aquelas que necessitam. Estes fornecedores não podem, em caso algum, divulgar informação sem autorização prévia de Ciências, não devem ter acesso a informação classificada como interna e não podem ter acesso a informação classificada como confidencial. Os fornecedores são ainda obrigados a respeitar todas as regras impostas pela instituição, assim como cumprir as políticas incluídas no presente documento.

Política de Desenvolvimento Seguro

Todos os programas desenvolvidos para Ciências devem ter em conta as boas práticas de programação. Aliado a isto, tudo o que seja produzido pela equipa de desenvolvimento da instituição deve ser implementado num ambiente isolado, composto preferencialmente por máquinas virtuais para permitir fazer separação de projetos e de forma a manter o sistema operativo do anfitrião (do inglês *hypervisor*) o mais limpo possível. Estas máquinas virtuais devem ainda estar numa rede dedicada ao desenvolvimento e com barreiras na Firewall.

Durante o desenho do produto, a equipa de desenvolvimento deve ter em consideração os princípios de Saltzer e Schroeder[1], de modo a minimizar possíveis vulnerabilidades.

O desenvolvimento seguro engloba a necessidade de criação de meios que permitam garantir a confidencialidade e integridade dos dados usados no produto final, assim como a disponibilidade do programa. É necessário ainda garantir que é possível autenticar e autorizar utentes, assim como desenvolver métodos que tornem possíveis a realização de auditorias e recolha de logs.

Na verificação dos programas produzidos, devem ainda ser incluídos os testes funcionais, de interface e de segurança, usando para tal dados de teste, que podem ser uma cópias de dados reais se o programa em questão não precisar de acesso à rede. Caso as aplicações usem dados classificados como confidenciais, deve ser emitido um relatório de testes de segurança.

A responsabilidade do desenvolvimento de programas, dos testes e dos dados utilizados para esses testes fica a cargo da equipa de desenvolvimento de Ciências.

[1]Princípios de segurança, descritos por Jerome Saltzer e Michael Schoeder. Os princípios referidos são economia de mecanismos, predefinições seguras, mediação completa, desenho aberto, separação de privilégios, privilégio mínimo, mínimo mecanismo em comum e aceitabilidade psicológica

Política de Destruição

Todos os documentos em suporte físico devem ser destruídos utilizando qualquer tipo de equipamento ou método que garanta a eficaz inutilização da informação neles contida.

Os equipamentos que contenham informação em suporte digital devem ser cedidos, em mão, aos serviços técnicos, responsáveis pela destruição dos equipamentos.

De referir que toda a documentação que não tenha nem possa vir a ter utilidade prática deve ser destruída.

Política de Dispositivos Móveis e Teletrabalho

A instituição pode fornecer aos utentes, e para cumprimento das funções associadas, dispositivos móveis como por exemplo computadores portáteis, sendo que os utentes responsáveis devem zelar por tais equipamentos, nunca os deixando sem supervisão. Dispositivos atribuídos a uma unidade podem ser usados por qualquer utente que pertença a essa mesma unidade, mas nunca podem conter informação classificada como confidencial. A configuração destes equipamentos fica a cargo da direção de serviços informáticos, mais especificamente da equipa de suporte ao utilizador.

Ciências permite que os seus utentes trabalhem remotamente, garantindo uma conexão segura à instituição através de uma ligação VPN. Assim são garantidas as propriedades de confidencialidade e integridade da informação dos utentes. Os utentes devem ter acesso apenas às funcionalidades necessárias para o desempenho das suas funções. Os utilizadores do serviço VPN devem garantir que a máquina que usam para a ligação não tem nenhum tipo de software malicioso que possa prejudicar a instituição.

Os computadores que se destinem a ser usados fora das instalações de Ciências, e que contenham informação classificada como confidencial devem ter o disco rígido cifrado usando um programa adequado para tal, sendo que deve existir uma cópia de segurança das chaves geradas na Direção de serviços informáticos. Os algoritmos de cifra permitidos deverão exibir robustez equivalente ou superior a:

- 3DES com chaves de 56 bits
- RSA com chaves no mínimo de 1024 bits
- AES com chaves no mínimo de 256 bits
- Twofish com chaves no mínimo de 128 bits

Se o computador pessoal for usado para guardar informação confidencial não é necessário cifrar todo o disco, mas criar uma partição cifrada para alojar tal informação.

Política de Gestão de Desastres

Esta política define requisitos básicos para fazer a gestão de desastres que possam ocorrer em Ciências. Para isto, a DSI define um plano de prevenção de falhas, um plano de contingência e um plano de recuperação de desastres, todos eles considerando um leque tão variado quanto possível de cenários.

Estes documentos devem existir tanto em suporte digital como em suporte físico e permanecer em local adequadamente divulgado à totalidade da equipa.

Plano de Prevenção de Falhas

Deve identificar os serviços vitais da instituição, assim como ameaças prováveis e medidas a tomar para mitigar tais ameaças.

O documento deve, para cada serviço, enumerar os vários tipos de ameaças e ação a tomar de forma a resolver cada uma dessas ameaças, assim como a equipa responsável por eliminar a ameaça. Este plano deve ser revisto a cada seis meses, de forma a incluir novos serviços e novos tipos de ameaças.

Plano de Contingência

O objetivo deste plano é diminuir o tempo de resposta a desastres e agilizar as ações de resposta.

Para os cenários definidos, e para cada serviço, deve listar vários tipos de situações, e para cada uma fornecer um procedimento a executar para resolver a situação. Deve ser atribuída uma equipa responsável à resolução do problema e um responsável principal. Deve ainda ser definido para cada situação, o impacto que representa para a instituição (alta, média ou baixa) e a prioridade. Este plano deve ser revisto e parcialmente testado semestralmente, e tendo em conta a criticidade do serviço em questão.

Plano de Recuperação de Desastres

O objetivo deste documento é a rápida e eficaz recuperação dos SI de Ciências em caso de desastre ou situação de emergência, reduzindo o tempo que os serviços estão paralisados

Tal como o plano de contingência, deve definir vários tipos de situações para cada serviço, apresentando um procedimento de resolução e mitigação do impacto para cada cenário. Deve ainda definir a equipa responsável pela resolução, o responsável principal, e a prioridade.

Política de Gestão de Incidentes de Segurança

Um incidente de segurança de informação é qualquer evento que possa afetar a confidencialidade, integridade ou disponibilidade dos dados de Ciências.

Sempre que seja detetado alguma anomalia em relação à segurança lógica da infraestrutura da instituição, esta deve ser comunicada de forma imediata à DSI através dos contactos fornecidos neste documento.

Os elementos da DSI envolvidos na análise do problema devem verificar a autenticidade deste problema, tentar resolvê-lo e posteriormente proceder à sua documentação se tal se justificar.

A DSI possui uma plataforma para registo e documentação de incidentes, onde estão presentes modelos de relatórios, assim como instruções para preenchimento de relatórios de incidentes, o que é útil para auditorias, mas mais importante, para que se possa ter uma reação mais rápida a incidentes que tendem a repetir-se.

Em situações mais graves é aconselhável solicitar os serviços do CERT.PT, entidade que coordena a resposta a incidentes de cibersegurança em Portugal. Os contactos desta entidade estão detalhados nos contactos disponíveis neste documento, para onde deve ser enviado uma mensagem de correio eletrónico que descreva detalhadamente o incidente.

Política de Palavra Passe

Todos os utentes de Ciências devem ter uma palavra passe pessoal e intransmissível, com validade máxima de 12 meses e cuja combinação de carateres tem obrigatoriamente que respeitar o seguinte conjunto de regras, que são verificadas pelo sistema aquando da alteração da mesma:

• Não contenham três ou mais caracteres consecutivos iguais ao nome de utilizador ou nome completo;

• Contenha pelo menos 6 caracteres;

• Deverá cumprir pelo menos três das seguintes quatro regras:

- Caracteres com letras maiúsculas (A..Z);
- Caracteres com letras minúsculas (a..z);
- Um ou mais algarismos (0..9);
- Caracteres não alfabéticos (!,$,#,&,...);

Após a expiração da palavra passe esta terá de ser reativada utilizando os mecanismos de recuperação da palavra passe (que devem ser configurados previamente pelos utilizadores), diretamente na Direção de Serviços Informáticos. No último caso, o pedido deve ser acompanhado da identificação do utilizador através do cartão de aluno/funcionário e/ou bilhete de identidade, carta de condução ou outro documento que identifique inequivocamente o utilizador.

Devem existir mecanismos que obriguem os utentes a alterar a palavra passe. Para além disto, não deve ser possível reutilizar qualquer uma das três palavras passe anteriores. A partir de quinze dias antes da data de expiração da palavra passe serão enviados automaticamente lembretes para o endereço de correio eletrónico registado do utilizador.

A palavra passe não pode ser guardada em claro, pelo que devem ser implementados mecanismos seguros para a salvaguarda das palavras passe dos utentes de Ciências, e ainda que esta instituição não pode solicitar a palavra passe aos utilizadores, sendo que isto deve ser amplamente comunicado aos utilizadores e de forma proactiva.

Política de Salvaguarda de Informação

É responsabilidade da Direção de Serviços Informáticos assegurar a disponibilidade de cópias de segurança dos dados mantidos pelos diferentes serviços, providenciando a sua disponibilidade na eventualidade de eliminação ou corrupção acidental ou intencional, falha de sistema ou desastres naturais.

O nível de criticidade de uma cópia de segurança depende diretamente dos dados que contém. É necessário que exista um procedimento que especifique como é feito o cálculo do valor de determinada informação, com base em critérios bem definidos e adaptados a Ciências.

Deve também existir um procedimento que defina o período de rotação e retenção das tapes, que defina ainda os dados e serviços a serem incluídos nas cópias de segurança e a frequência com que tais cópias são efetuadas, com base na criticidade dos dados. Deve ainda ser definida uma convenção bem definida para etiquetar todas as tapes de forma a permitir uma identificação intuitiva. As cópias de segurança existentes devem ser de recuperação imediata ou de arquivo.

Deve existir um procedimento que descreva o processo de verificação das cópias de segurança, a realizar com periocidade definida previamente.

É também imperativo que sejam alojadas numa localização geográfica diferente de Ciências tapes capazes de reestabelecer a infraestrutura lógica da instituição.

Política de Proteção Individual dos Dados

De acordo com a ISO 27001, não devem ser deixados sobre as secretárias dispositivos de armazenamento removíveis durante a ausência dos funcionários, assim como inserir nas máquinas/rede de Ciências dispositivos que tenham sido (ou se suspeite que tenham sido) manuseados por desconhecidos. Tais dispositivos devem ser entregues na DSI.

Todas as máquinas dentro da DSI devem ser desligadas no final do dia de trabalho e, durante a ausência do local de trabalho, os funcionários da DSI devem sempre bloquear as máquinas. Estas devem ainda ser configuradas para bloquearem automaticamente dentro de quinze minutos (máximo), período após o qual, apenas podem ser desbloqueadas introduzindo a senha.

Política de Gestão de Chaves Criptográficas

O processo de gestão de chaves criptográficas deve ter em conta a utilização de tais chaves, isto é, qual a sua finalidade, a proteção e a vida útil. As chaves criptográficas devem ser usadas para cifrar documentos classificados como confidenciais que necessitem de ser transferidos. Todas as chaves devem ser geradas e armazenadas num servidor dedicado e que deve estar devidamente protegido contra acesso e modificação não autorizados.

Todos os certificados de Ciências devem expirar ao fim de três anos ou antes, se comprometidos ou se suspeite que possam ser comprometidos.

Política de Transferência e Armazenamento Pessoal de Informação

Esta política define métodos para a transferência controlada de informação de Ciências. Estes métodos incluem o uso de protocolos seguros, assim como o uso de procedimentos claros para o efeito.

O correio eletrónico de Ciências deve ser utilizado segundo as regras definidas nesta política para que a imagem da instituição seja preservada, sendo que estas regras aplicam-se a todos os utentes da instituição. O sistema de correio eletrónico de Ciências não pode ser usado para fins contraditórios com a missão da instituição.

O envio de correio eletrónico para um número elevado de utilizadores deve ser feito através de listas de correio eletrónico. Os membros de cada lista são informação confidencial e da responsabilidade de quem gere essa mesma lista.

A instituição deve ainda permitir mas desencorajar os seus utilizadores (exceto alunos) de redirecionar correio eletrónico para outras contas, incluindo contas externas, assim como deve permitir a criação de respostas automáticas.

Adicionalmente é obrigatória a utilização de filtros que impeçam o acesso imediato e nas mesmas condições de mensagens marcadas como legítimas a mensagens recebidas consideradas inválidas (vírus, *spam*, *phishing*), contribuindo desta forma para a economia de recursos e tempo e para a segurança da rede. Paralelamente, os utentes da instituição não devem abrir qualquer tipo de anexo associado a mensagens cujo endereço de correio eletrónico de origem seja desconhecido.

Os protocolos de envio/receção de correio eletrónico permitidos são POP3S, IMAP4S, SMTPS e MAPI.

Devem também ser implementados mecanismos que permitam o envio de correio eletrónico cifrado e/ou assinado.

Os utentes de Ciências podem também fazer uso de outros serviços de armazenamento em nuvem, nomeadamente externos, desde que guardem apenas informação classificada como pública. Informação classificada acima desta categoria deve ser armazenada exclusivamente na instituição.

A impressão de todos os documentos cuja informação esteja classificada como confidencial tem de ser supervisionada pelo responsável pela informação.

Relativamente a dispositivos amovíveis, Ciências permite aos seus utentes que liguem os seus dispositivos pessoais às máquinas da instituição desde que se responsabilizem por qualquer dano que tais dispositivos possam causar. No entanto, é expressamente proibido ligar qualquer tipo de dispositivo amovível que tenha sido encontrado. Estes devem ser entregues na Central de Segurança ou na Direção de serviços informáticos.

É permitido à equipa de suporte ao utilizador usar dispositivos amovíveis para distribuição de programas dentro da instituição, desde que no contexto da missão de Ciências.

Não é permitido o uso de meios amovíveis para transporte de informação confidencial.

Acrónimos

3DES – Triple Data Encryption Standard

AES - Advanced Encryption Standard

DSI – Direção de Serviços Informáticos

IMAP4S – Internet Message Access Protocol 4 Secure

ISO - International Organization for Standardization

MAPI - Messaging Application Programming Interface

POP3S – Post Office Protocol 3 Secure

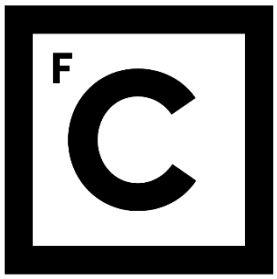
RSA – Algoritmo Rivest, Shamir, Adleman

SI – Sistemas de Informação

SMTPS - Simple Mail Transfer Protocol Secure

VPN - Virtual Private Network

PROCEDIMENTOS DE SEGURANÇA DE INFORMAÇÃO



Ciências
ULisboa

Faculdade
de Ciências
da Universidade
de Lisboa

Classificação:	Interno
Código do Documento:	Proced_DSI
Versão do Documento:	1.2
Data da Última Revisão:	26 de Setembro de 2016
Elaborado por:	João Matias – Direção de Serviços Informáticos
Verificado por:	Hugo Miranda - Coordenador da Direção de Serviços Informáticos

Índice

Introdução

Este documento descreve os procedimentos a seguir pelos utentes da Faculdade de Ciências da Universidade de Lisboa para garantir a de segurança e confidencialidade da informação.

Estes procedimentos estão de acordo com a norma ISO 27001:2013 e com as Políticas de Segurança de Informação definidas para a instituição no documento "Políticas de Segurança de Informação".

Informação de Contactos

DIREÇÃO DE SERVIÇOS INFORMÁTICOS

Faculdade de Ciências da Universidade de Lisboa

Edifício C1, Piso 2, Sala 1.2.10

Campo Grande 1749-016

Lisboa

Telefone Geral: 217 500 000

Extensão Interna: 21248

Correio Eletrónico: suporte@ciencias.ulisboa.pt

Procedimento para Acesso à Rede Física

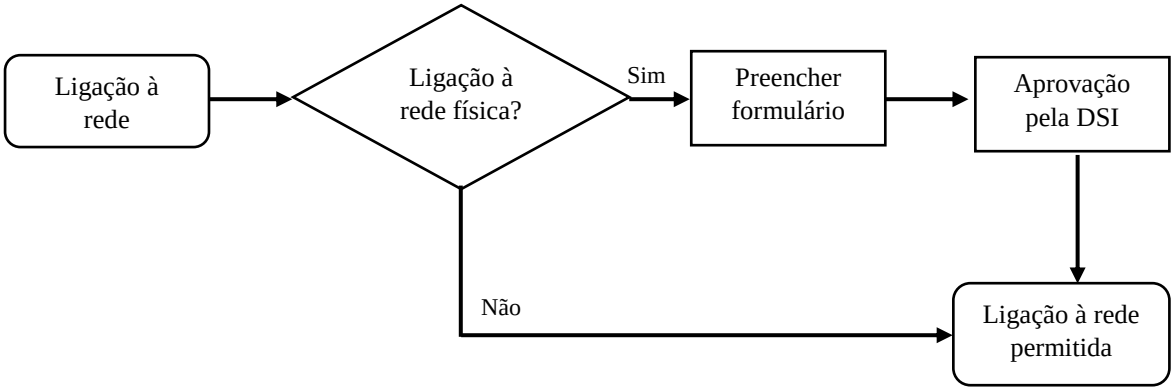
Utilizador: Utente de Ciências ou Visitante

Intervenientes: Suporte Operacional

Procedimento:

O acesso à rede cablada é reservado exclusivamente a utentes de Ciências, sendo necessário que os utentes solicitem um ativação de tomada de rede, preenchendo o formulário disponível na plataforma da instituição, usando os seus dados pessoais e os dados do equipamento que pretendem ligar à rede. Os utentes devem ter conhecimento das políticas de segurança associadas, disponíveis na plataforma da instituição.

Fluxograma:



Procedimento para Alteração de Palavra Passe

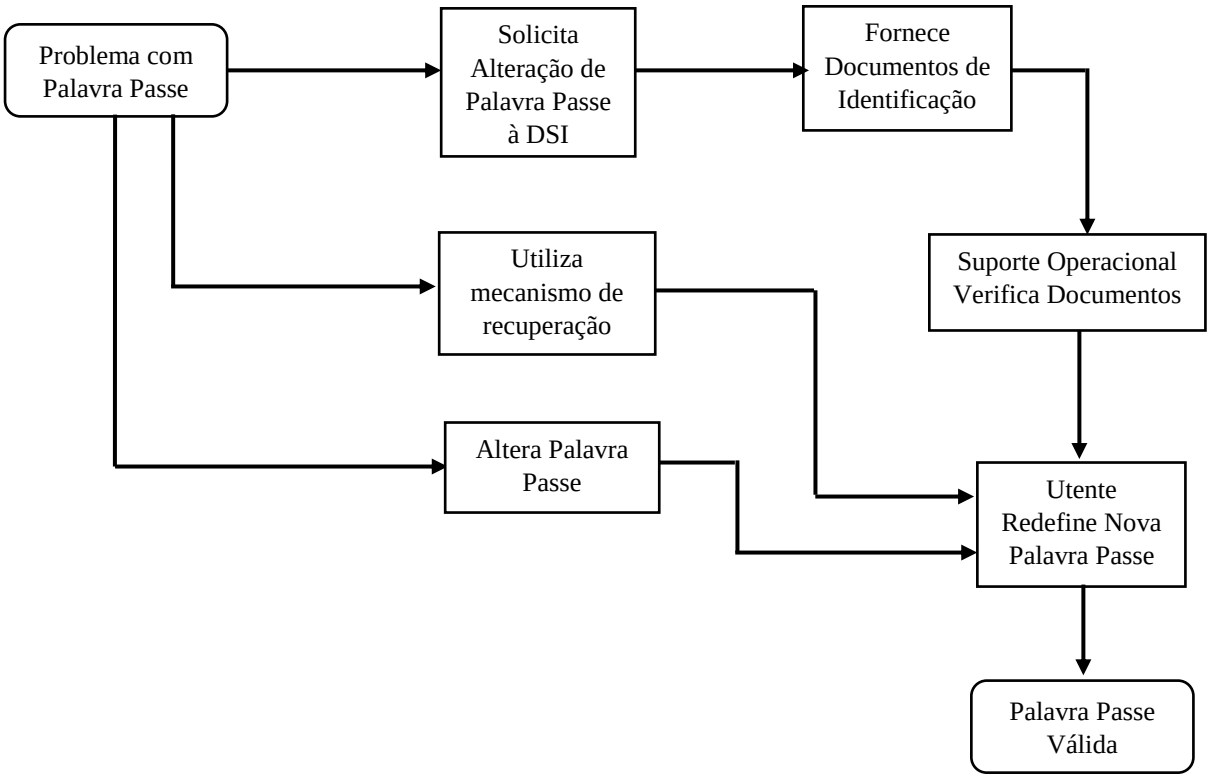
Utilizador: Utente de Ciências

Intervenientes: Suporte Operacional

Procedimento:

Caso um utente se esqueça da sua palavra passe, esta tenha expirado ou tenha sido comprometida, deve dirigir-se à DSI e informar a equipa de suporte ao utilizador ou alterá-la através dos mecanismos existentes. O utente deverá identificar-se perante o elemento da equipa de suporte operacional, através de um documento pessoal[1], sendo o elemento da equipa responsável por validar a identidade. A equipa de suporte deve dar acesso à funcionalidade de redefinição da palavra passe do utente, sendo que este processo deve ser executado com a maior brevidade possível.

Fluxograma:



[1] Este documento poderá ser o cartão de aluno/funcionário e/ou bilhete de identidade, carta de condução ou outro documento oficial com fotografia que identifique inequivocamente o utilizador.

Procedimento para Gestão de Incidentes de Segurança

Utilizador: Utente de Ciências

Intervenientes: Suporte Operacional

Procedimento:

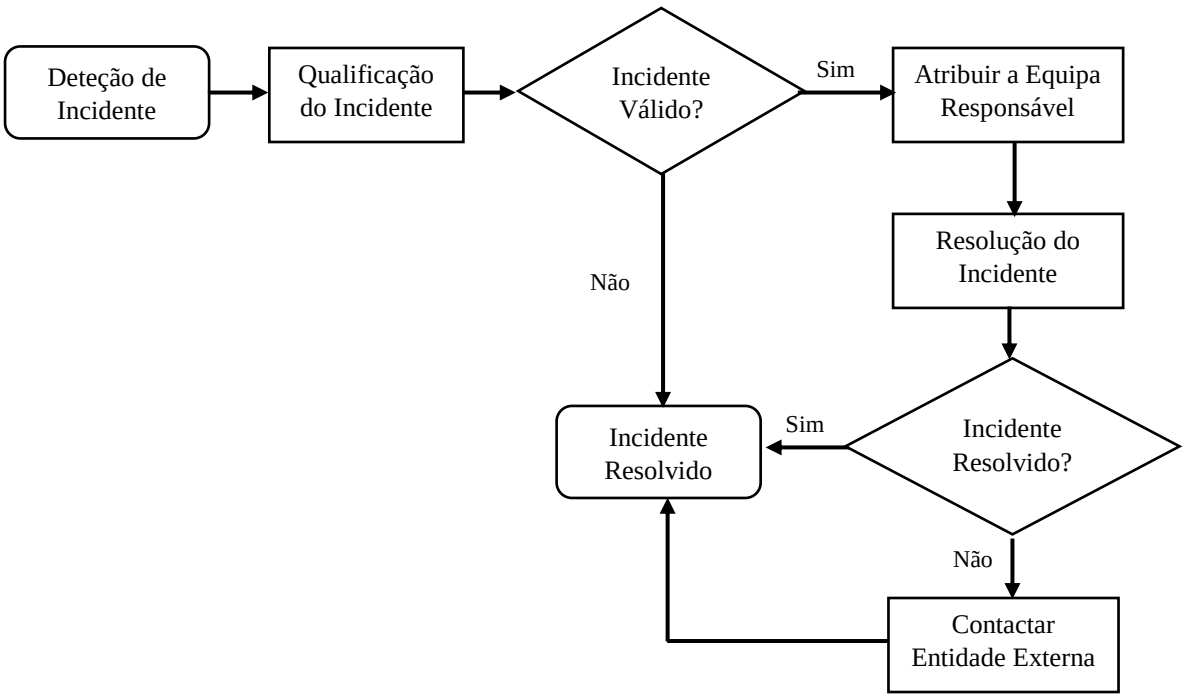
Os utentes devem reportar todos os incidentes ou suspeitas relacionados com os Sistemas de Informação de Ciências ao suporte operacional. A equipa de suporte deve fazer a qualificação do incidente, avaliando o risco resultante para a instituição. Se a situação assim o justificar, a resolução do incidente deve ser atribuída à equipa da DSI da área técnica onde tal incidente se enquadra.

Em situações extremas, em que a equipa da DSI responsável pela resolução do incidente não esteja preparada para resolver a situação, deve então ser contactada uma entidade externa habilitada para tal tipo de cenários, como é o caso do Centro Nacional de Cibersegurança. Esta ação deve ser aprovada pelo coordenador da DSI.

Toda a informação acerca do incidente deve ser documentada na plataforma existente para o efeito, para que a resolução de situações semelhantes, no futuro, seja mais rápida e eficaz.

A DSI deve ter ativos mecanismos para deteção e geração de alertas.

Fluxograma:



Procedimento para Definição de Valor da Informação

Utilizador: Utente de Ciências

Intervenientes: -

Procedimento:

Para atribuir um valor, mesmo que qualitativo, a determinada informação é necessário ter definidas métricas relativamente à confidencialidade, integridade e disponibilidade dessa informação.

Assim, e relativamente à confidencialidade define-se como **informação confidencial**, aquela que só deve estar acessível aos administradores de sistemas ou aos gestores da informação, **informação interna** se acessível apenas por utentes e **informação pública** se acessível por qualquer utilizador. A Tabela 1 define as correspondências numéricas para a confidencialidade.

Relativamente à integridade, define-se informação com **integridade negligenciável** se a alteração dos dados é aceitável, sendo que não representa danos para a instituição se a alteração não é detetada, **integridade marginal** se a alteração é aceitável mas percetível e recuperável **integridade crítica** se a alteração é inaceitável, representando danos para a instituição. A Tabela 2 define as correspondências numéricas para a integridade.

Por fim, e relativamente à disponibilidade, define-se a informação com **indisponibilidade aceitável** se a sua disponibilidade por um período de até 7 dias consecutivos, **indisponibilidade pontual** até 24 horas, **indisponibilidade reduzida** até 8 horas e **indisponibilidade inaceitável** até 88 horas num ano. A Tabela 3 define as correspondências numéricas para disponibilidade.

O valor de informação (VI) é definido utilizando os pesos atribuídos a cada propriedade de acordo com a fórmula:

$$VI = \frac{2 \times [INTEGRIDADE] + [CONFIDENCIALIDADE] + [DISPONIBILIDADE]}{4}$$

A Tabela 4 define o valor da informação em função da pontuação atribuída..

Integridade	**Pontuação**
Negligenciável	1
Marginal	2
Crítica	3

Tabela 1: Níveis de Integridade

Confidencialidade	**Pontuação**
Pública	1
Interna	2
Confidencial	3

Tabela 2: Níveis de Confidencialidade

Disponibilidade	**Pontuação**
Indisponibilidade aceitável	1
Indisponibilidade pontual	2
Indisponibilidade reduzida	3
Indisponibilidade inaceitável	4

Tabela 3: Níveis de Disponibilidade

Valor da Informação	**Pontuação**
Marginal	$V \leq 1{,}9$
Médio	$1{,}9 \leq V < 2{,}9$
Relevante	$2{,}9 \leq V < 3{,}4$
Crítico	$V \geq 3{,}9$

Tabela 4: Valor da Informação

Procedimento para Destruição de Informação

Utilizador: Utente de Ciências

Intervenientes: Serviços Técnicos

Procedimento:

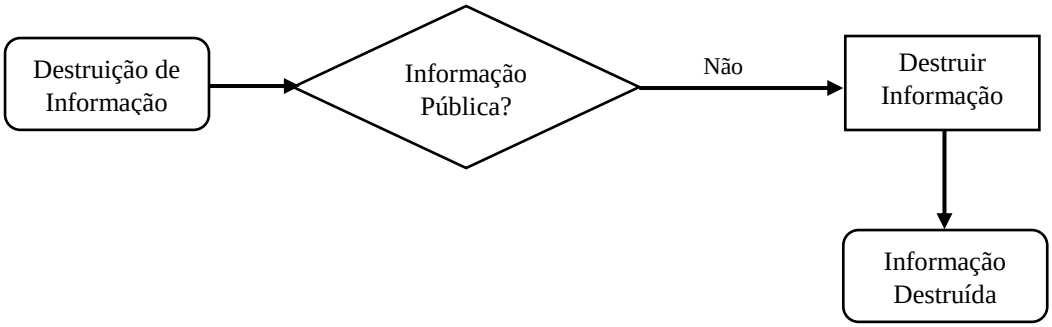
Os documentos que contenham informação classificada acima de pública, isto é, interna ou confidencial, têm necessariamente que ser destruídos fisicamente, quer a informação se encontre em suporte físico ou digital.

Para proceder à destruição de documentos em papel classificados como proprietários, restritos ou confidenciais deverá ser usada uma destruidora de papel.

Relativamente à informação em suporte digital, todos os dispositivos que armazenem informação classificada como interna ou confidencial devem ser entregues pelo responsável aos Serviços Técnicos, encarregues por fazer a destruição. De igual forma, meios de armazenamento no fim de vida útil devem ser entregues aos Serviços Técnicos para destruição, considerando-se que o procedimento a adotar deve ser o imposto à informação com classificação mais elevada que ele possa conter.

É obrigatório que seja feito o registo da entrega e aceitação do suporte pelo membro do Gabinete de Infraestruturas e Apoio Técnico (GIAT) e à manutenção do suporte em local com acesso reservado até que o suporte seja efetivamene destruido.

Fluxograma:



Procedimento para Realização de Cópia de Segurança

Utilizador: Equipa de Administração de Sistemas de Ciências.

Intervenientes: -

Procedimento:

A equipa de administração de sistemas de Ciências é responsável por gerir todo o processo de cópia de segurança[2] para salvaguarda da informação pertencente a Ciências. Os equipamentos que realizam tais cópias devem encontrar-se em local de acesso restrito.

A informação é salvaguardada utilizando cópias completas e incrementais. O documento Cópias de Segurança contém uma tabela que apresenta valores de referência para a frequência e retenção das cópias de segurança de acordo com a classificação da informação, assim como frequência de verificação de integridade de dados e o local onde devem ser armazenadas.

As tapes devem ser identificadas através da notação FC seguida de 4 dígitos, formando assim um número de série que cresce de forma sequencial. Esta identificação deve estar presente na tape. Deve ainda ser usado uma aplicação capaz de gerir todo o processo de gestão de cópias de segurança, e que permita identificar o tipo de cópia contido em cada tape.

O processo de limpeza do equipamento de cópia de segurança deve ser efetuado quando a aplicação que gere o *robot* o solicita.

[2] Do inglês “backup”

Procedimento para Criar e Eliminar Utilizadores

Utilizador: Utente de Ciências

Intervenientes: Suporte Operacional

Procedimento:

As contas de utilizadores de Ciências dividem-se em dois domínios, @ciencias.ulisboa.pt e @alunos.ciencias.ulisboa.pt. No primeiro domínio são incluídos os docentes, investigadores, bolseiros e funcionários. No segundo são incluídos os alunos e utilizadores com ligação temporária à instituição.

As contas dos alunos podem ser atribuídas a partir do dia da inscrição e as restantes a partir do primeiro dia de contrato, ambas pelo suporte operacional.

Contas de utilizadores temporários

As contas de utilizador temporárias destinam-se a grupos de utilizadores externos para que consigam ter acesso aos serviços fornecidos por Ciências. É necessário que um Docente, Investigador ou Funcionário fique responsável por esta conta.

Existem dois tipos de conta temporária: Conferência e Visitante. A conta de conferência pode ser equiparada à conta de aluno, com a exceção que pode ser partilhada por um grupo de utilizadores. Em relação à conta de visitante, tem os mesmos privilégios que uma conta de funcionário e é obrigatoriamente individual.

Estas contas podem ter duração prorrogável de 2, 5, 8, 15 ou 30 dias a decidir por quem faz o pedido de criação de conta, o nome do utilizador é gerado com base no nome do requerente e é atribuída uma palavra passe temporária, que terá que ser alterada pelo utilizador.

Procedimento para Teletrabalho

Utilizador: Utente de Ciências

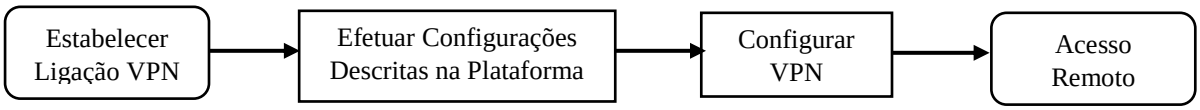
Intervenientes: Equipa de Redes de Ciências

Procedimento:

Para se ligarem remotamente à rede interna de Ciências, os utentes devem estabelecer uma ligação de Rede Privada Virtual (VPN) que assegura a confidencialidade de informação trocada entre a infraestrutura de Ciências e o equipamento utilizado remotamente pelo utilizador. Para tal, os utentes devem seguir os passos de configuração da VPN descritos na plataforma da instituição. As configurações de VPN existentes foram definidas pela equipa de redes, pelo que qualquer questão ou problema relacionado com a ligação VPN deve ser endereçada a esta equipa e para tal, os utilizadores devem dirigir-se ao suporte informático.

Os equipamentos utilizados para se ligarem à VPN são obrigados a respeitar todas as políticas definidas pela instituição.

Fluxograma:



Procedimento de Testes de Eletricidade

Utilizador: Equipa de Administração de Sistemas e Redes de Ciências

Intervenientes: -

Procedimento:

Devem ser executados, regularmente, testes ao gerador de Ciências e às UPS de forma a garantir o correto funcionamento destes equipamentos.

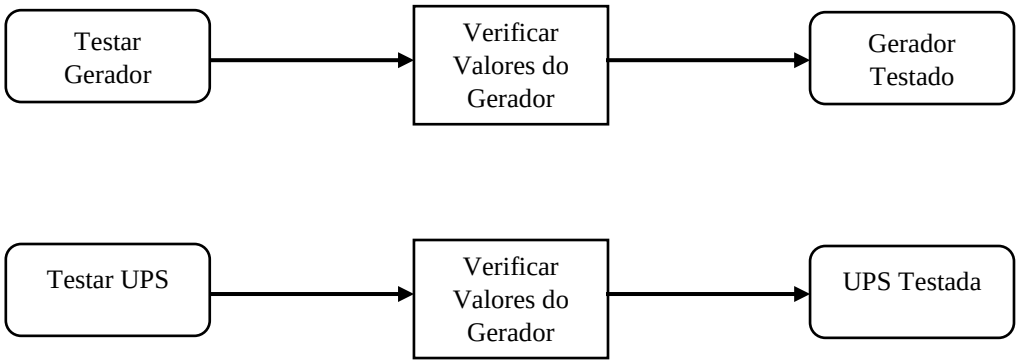
Testes ao Gerador

O gerador de Ciências deve ser testado a cada dois meses, sendo necessário verificar o correto funcionamento do equipamento, o nível de combustível, água e a tensão de saída.

Testes às UPS

As UPS de Ciências devem ser testado a cada dois meses, sendo necessário verificar o correto funcionamento dos equipamentos, a tensão de saída e os avisos presentes no ecrã do equipamento.

Fluxograma:



Procedimento de Testes de Backup

Utilizador: Equipa de Administração de Sistemas e Redes de Ciências

Intervenientes: -

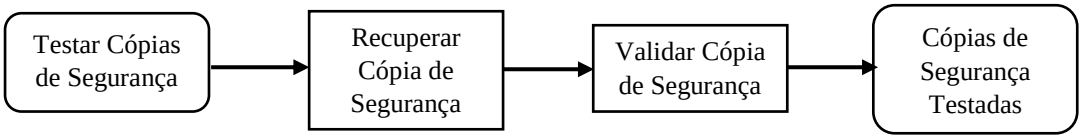
Procedimento:

O sistema de cópias de segurança deve ser testado frequentemente de forma a garantir o correto funcionamento deste sistema.

Testes ao sistema de Cópias de Seguranças

Devem ser realizados testes às cópias de segurança uma vez por mês, de forma a expor possíveis problemas com o *robot*, com as tapes ou com os procedimentos de armazenamento. A cada mês devem ser testados todas as combinações de tipos e locais de armazenamento diferentes. Para testar uma cópia de segurança, basta proceder à sua recuperação e validar a integridade dos dados, sendo que no final deste processo, deve ser elaborado um relatório.

Fluxograma:



Acrónimos

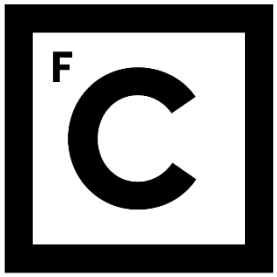
ISO - International Organization for Standardization

DSI – Direção de serviços informáticos

VPN - Virtual Private Network

UPS - Uninterruptible Power Supply

PLANO DE CONTINGÊNCIA



Ciências
ULisboa

Faculdade
de Ciências
da Universidade
de Lisboa

Classificação:	Confidencial
Código do Documento:	PC_DSI
Versão do Documento:	1.1
Data da Última Revisão:	26 de Setembro de 2016
Elaborado por:	João Matias – Direção de Serviços Informáticos
Verificado por:	Hugo Miranda - Coordenador da Direção de Serviços Informáticos

Índice

Introdução

O Plano de Contingência descreve como proceder perante situações adversas e identificadas antecipadamente. Este documento é constituído por diversos cenários, cada um com um conjunto de procedimentos a ser executados, sendo também atribuídas responsabilidades específicas aos diferentes núcleos da DSI.

O presente documento deve ser revisto e testado semestralmente.

Informação de Contactos

Números Internos

Unidade	Nome	Extensão
Direção	Dirce Monteiro Assis	25426
Unidade de Infraestruturas e Apoio Técnico	José Fernandes	24135
Central de Segurança		25505

Números Externos

Entidade	Número
Regimento de Sapadores de Bombeiros	+351218171431

Serviço: Datacenter

Evento: Incêndio

Procedimento

Evacuar pessoas que se encontrem dentro do Datacenter

Desligar corrente elétrica que alimenta o Datacenter

- Localizar os quadros de corte geral, à esquerda da porta de acesso ao Datacenter
- Desligar todos os interruptores associados à etiqueta “CORTE GERAL”

Contactar Central de Seguranças

Ativar mecanismos de extinção de incêndios

Documentar evento

Equipa Responsável

Direção de Serviços Informáticos - Equipa de Administração de Sistemas e Redes

Evento: Acesso físico não autorizado

Procedimento

Analisar *logs* de acesso

Bloquear acesso virtual aos serviços afetados

Analisar *logs* dos serviços afetados

Listar informação acedida, modificada e/ou eliminada

Documentar evento

Equipa Responsável

Direção de Serviços Informáticos - Equipa de Administração de Sistemas e Redes

Serviço: Software de Virtualização

Evento: Escassez de recursos

Procedimento

Desligar serviços menos críticos

Fazer levantamento de recursos necessários e respetivas especificações

Estimar o custo esperado para perceber se o orçamento atribuído é suficiente

Iniciar processo de aquisição de recursos

Reativar serviços menos críticos

Equipa Responsável

Direção de Serviços Informáticos - Equipas de Administração de Sistemas e de Redes

Evento: Comprometimento do Hypervisor

Procedimento

Notificar todos os utilizadores que o serviço vai ser suspenso

Suspender todos os serviços fornecidos pelas máquinas virtuais alojadas no Hypervisor

Desligar todas as máquinas virtuais alojadas no Hypervisor

Analisar *logs* para avaliar danos

Corrigir falha do Hypervisor que permitiu o incidente

Notificar utentes da situação, se tal se justificar

Documentar evento

Solicitar colaboração do CERT, se tal se justificar

Equipa Responsável

Direção de Serviços Informáticos - Equipa de Administração de Sistemas e Redes e de Suporte ao Utilizador

Serviço: Alojamento de Páginas Web

Evento: Defacement

Procedimento

Exibir página temporária de manutenção para a página afetada

Bloquear acessos à página afetada

Analisar *logs* de acesso

Documentar evento

Solicitar colaboração do CERT

Equipa Responsável

Direção de Serviços Informáticos - Equipa de Administração de Sistemas e Redes

Evento: SQL Injection

Procedimento

Bloquear acesso à base de dados em questão, definindo permissões de acesso apenas para administradores de sistemas

Analisar *logs* de acesso e da base de dados

Listar informação acedida, modificada e/ou eliminada

Documentar evento

Equipa Responsável

Direção de Serviços Informáticos - Equipa de Administração de Sistemas e Redes

Acrónimos

DSI – Direção de Serviços Informáticos